Informationssäkerhetshandbok

Ledningssystem för informationssäkerhet

Informationssäkerhetshandbok

Diarienummer:

Dokumentansvarig: Kommundirektören

Adresserat till: Samtliga medarbetare i Linköpings kommun

Tidpunkt för aktualitetsprövning: Årligen

Tidpunkt för senaste revidering: 2021-09-30

Relaterade styrdokument: Riktlinje för informationssäkerhet och Säkerhetspolicy

Sökord: LIS, handbok, informationssäkerhet, it-säkerhet, ramverk, säkerhet

Informationssäkerhetshandbok

Ledningssystem för informationssäkerhet

Revidering

	Datum	Ändring	Signatur
001	2021-08-15	Stavfel och tillägg: ordet chefsjurist	Alexis Holm, eLärandeCenter
002	2021-09-30	Uppdatering av förord + Datum	Alexis Holm, eLärandeCenter

Förord

Det här är en informationssäkerhetshandbok för Linköpings kommun vilken- har en direkt koppling till kommunens säkerhetspolicy samt riktlinje för informations-säkerhet. Handboken är en del av ledningssystem för informations-säkerhet, vilket anknyter till kommunens förvaltningsmodell för it-stöd.

Med denna handbok vill vi pedagogiskt presentera vad samtliga berörda i kommunen behöver veta samt på sikt göra, för att informationen ska hanteras i en kommungemensam informationssäkerhetsprocess. Med detta menas att den hanteras på ett sådant sätt att både vi själva och kommunens invånare känner tillit till att kommunens informationshantering lever upp till de krav och förväntningar som finns.

Implementeringen av handboken påbörjas under hösten 2021 och ska ske stegvis under flera år, med den slutliga målsättningen att ge vår information ett så bra skydd som möjligt på ett så likartat och smidigt sätt som möjligt. Det ska helt enkelt vara lätt att göra rätt.

Stora delar av den kommunala verksamheten styrs av lagar, förordningar och avtal som vi naturligtvis ska följa. Informationssäkerhetsarbetet påverkas mycket av offentlighets- och sekretesslagstiftningen och dataskyddslagstiftningen, men också av annan lagstiftning. Denna handbok täcker inte samtliga juridiska aspekter, utan handboken behöver läsas tillsammans med andra kommunala riktlinjer, tillämpningsanvisningar och handböcker. Dessutom består arbetet av bedömningar där olika åtgärder måste vägas mot varandra och mot övrig reglering. På så vis säkerställer vi att informationssäkerhetsarbetet i kommunen sker på ett korrekt sätt.

Området informationssäkerhet är inte alltid svart eller vitt – arbetet består ofta av bedömningar där man måste väga olika åtgärder mot varandra. Det allra viktigaste är att du som medarbetare är medveten om att det mesta du hanterar i din verksamhet faktiskt handlar om informationssäkerhet utifrån ett medvetet, eftertänksamt och praktiskt perspektiv – vem ska veta vad och på vilket sätt.

Paul Håkansson
Kommundirektör

2021-09-29

Innehåll

Kapitel 1 - Inleding

Linköpings kommuns Säkerhetspolicy samt dess tillhörande riktlinjer för info-rmationssäkerhet är övergripande dokument som redovisar kommunens övergripande mål för informationssäkerhet och inriktningen på detta arbete.

Från kommunens Säkerhetspolicy (målbild):
Informationssäkerhet är kommunens förmåga att hantera information så att legala, etiska och verksamhetsmässiga intentioner upprätthålls.

Denna handbok konkretiserar kommunens riktlinjer för informationssäkerhet med mer detaljerad information om regler och anvisningar för informationssäkerhet. Handboken baseras på den svenska respektive den internationella standarden för informationssäkerhet (SS-ISO/IEC 27001 respektive SS-ISO/IEC 27002) som Linköpings kommun eftersträvar att följa.

Denna handbok fastställs av kommundirektören i enlighet med vad kommunstyrelsen uppdragit åt kommundirektören.

1.1 Handbokens innehåll

Handboken innehåller beskrivningar, anvisningar och regler om säkerhet vid all hantering av information inom Linköpings kommun.

Handboken gäller Linköpings kommuns samtliga verksamheter. Det finns alltså inget utrymme för att besluta om lokala regler utom när så särskilt anges.

Intentionen är att handboken även ska kunna tillämpas i kommunens bolag för att dessa ska nå god informationssäkerhet. Respektive bolag beslutar dock om riktlinjer, regler och anvisningar etc. för informationssäkerhet inom respektive bolag. Delar av handboken gäller även externa aktörer när dessa använder sig av kommunens informationstillgångar eller om det finns särskilda behov av samordning.

Handboken är skriven med Linköpings kommuns verksamhet i fokus och behandlar generellt sett inte påverkan på annan part, såvida detta inte särskilt framgår.

1.2 Avgränsningar

Handboken är inriktad på informationssäkerhet och behandlar därmed inte -andra närliggande områden som t.ex. säkerhetsskydd och integritetsskydd.

Dessa verksamheter har egna organisationer och styrs främst utifrån lagar och förordningar. Om säkerhetsskydd och dataskydd integrerar med informationssäkerhetsarbetet framgår detta på vissa ställen i handboken. Handboken är dock ingen fullständig instruktion eller vägledning gällande säkerhetsskydd eller dataskydd.

Handboken ersätter inte lagar, förordningar och föreskrifter inom informationssäkerhetsområdet utan ska fungera som ett stöd för att tillämpa olika rättsliga krav i verksamheten.

1.3 Struktur och läsanvisningar

För att ge god läsbarhet är handboken uppdelad i sju kapitel (1–7) med olika innehåll som riktar sig till olika målgrupper. Viss information återupprepas dock, för att enstaka kapitel ska kunna läsas fristående.

> Informationssäkerhetshandboken är en källa där du kan söka information; du behöver inte läsa och förstå allt i handboken. Tänk på att viss information i handboken återupprepas för att enstaka kapitel ska kunna läsas fristående.

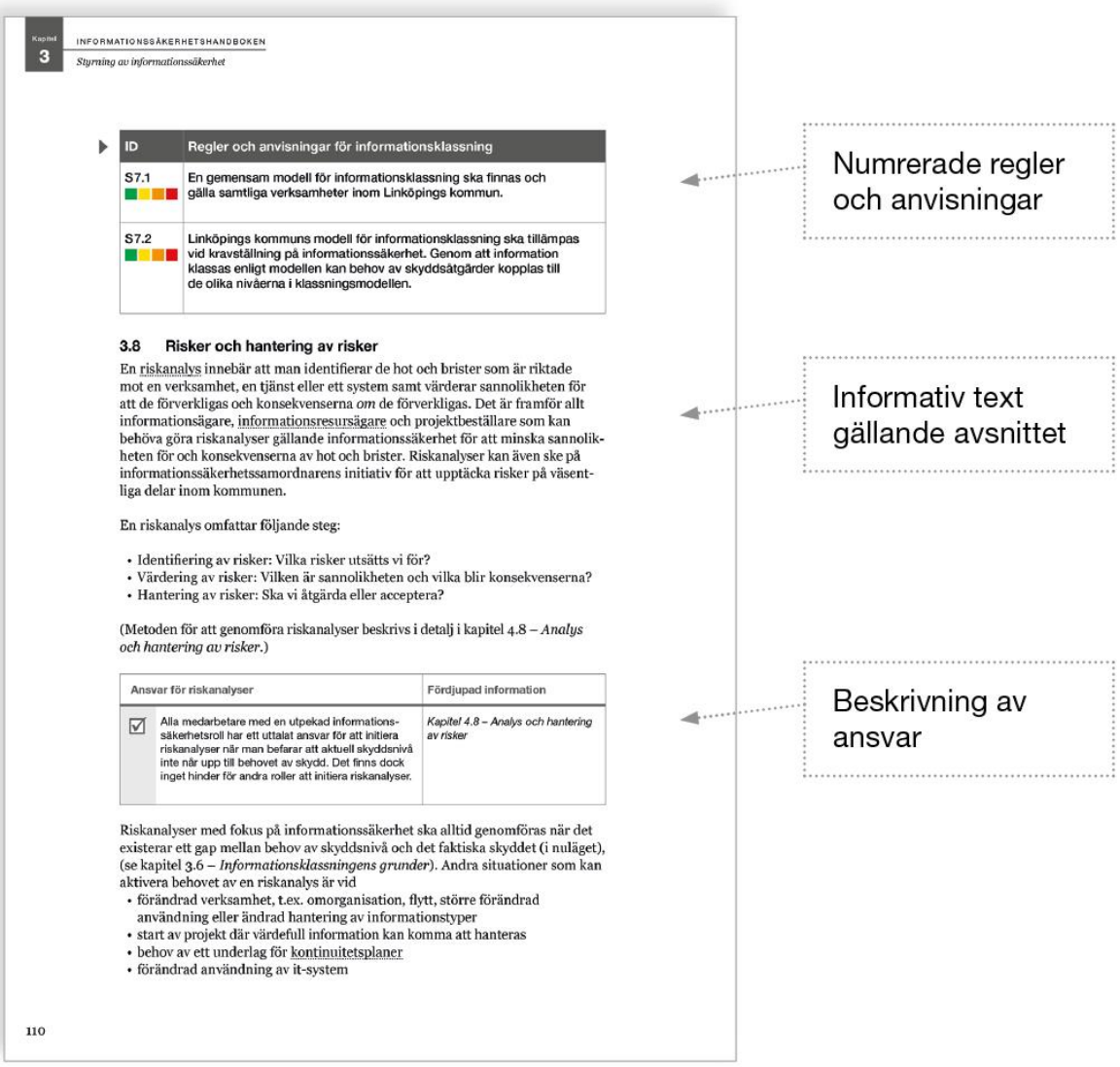
I tabell 1 nedan visas en översikt över samtliga kapitel i handboken. Samtliga medarbetare i kommunen bör fokusera på innehållet i de två första kapitlen. Resterande kapitel innehåller främst information riktad till chefer och medarbetare som har specifika roller i kommunens informationssäkerhetsarbete.

Kapitel	Innehåll	Primär målgrupp	Sidor
1. Inledning	Introduktion	Alla medarbetare	11-32
2. Informationssäkerhet för medarbetare	Information om samt anvisningar och regler för hur information ska hanteras i dagligt arbete.	Alla medarbetare och externa aktörer (som hanterar kommunens information)	33-78
3. Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information om samt anvisningar och regler för hur arbetet med informationssäkerhet ska bedrivas.	Chefer och alla som har en utpekad roll i kommunens informationssäkerhetsarbete	79-127
4. Informationssäkerhet i verksamhetsnära förvaltning	Information om och anvisningar och regler för chefer om informationssäkerhet i specifika förvaltningsobjekt, t.ex. system och grupper av system.	Chefer, informationsägare, objektägare verksamhet samt förvaltningsledare verksamhet	128-156
5. Informationssäkerhet i it-nära förvaltning	Information om samt anvisningar och regler för hur information och it ska hanteras inom it-miljön, dvs. it-säkerhet.	Objektägare it, förvaltningsledare it samt medarbetare i it-organisationen	157-192
6. Informationssäkerhet och fysiskt skydd	Information om samt regler och anvisningar för hur de fysiska skydden ska utformas för att skydda information.	Chefer, verksamhetansvariga, fastighetsansvariga, lokalansvariga, lokalstrateger, lokalplanerare	193-207
7. Begrepp och referenser	Termer, begrepp och länkar.	Alla medarbetare	208-222

Tabell 1. Struktur och läsanvisningar

1.4 Uppbyggnad av handboken, regler och anvisningar

Varje kapitel består dels av informativa avsnitt, dels av obligatoriska regler och anvisningar. Vanligen behandlas ett delområde i taget med informativ text som sedan följs av regler och anvisningar. Begrepp skrivs med understruken punktad markering första gången de används i handboken och begreppens förklaring återfinns i kapitel 7.1 – Begrepp och definitioner. I texten förekommer även kursiv stil som används vid hänsvisningar till andra avsnitt handboken. Kursiv stil används även vid förstärkningar, t.ex. när något i texten är extra viktigt.



Figur 1. Struktur i handboken. Bilden ett exempel som beskriver handbokens struktur. På bilden ser man en tabell med numrerade regler och anvisningar. Bilden pekar även på att ett textavsnitt ska innehålla informativ text gällande det specifika avsnittet. Längst ner i bilden syns en tabell med två kolumner, "Ansvar för riskanalyser" och "fördjupad information", denna del är en beskrivning av ansvar.

Samtliga regler och anvisningar är numrerade och återfinns i tabeller med tabellrubrik. Olika typer av information i kommunen kommer tilldelas informationsklasser (se även kapitel 3.7 – *Informationsklassning i Linköpings kommun*). Alla regler och anvisningar är grafiskt markerade för att visa när de är tillämpliga (för vilken informationsklass).

Informationsruta

Avsikten med nedanstående är att visa hur regler och anvisningar är uppbyggda. Texter i detta uppslag innehåller dock begrepp som ännu inte förklarats. Hur begrepp som skyddsbehov, skyddsnivåer och tillämpningar av dessa kopplas samman, förklaras senare i handboken. Om det är första gången du läser handboken, återkom hit när du läst de inledande avsnitten i kapitel 2 (se även förklaringar i kapitel 7).

Olika grafiska markeringar används i handboken för att tydliggöra hur regler och anvisningar ska tillämpas.

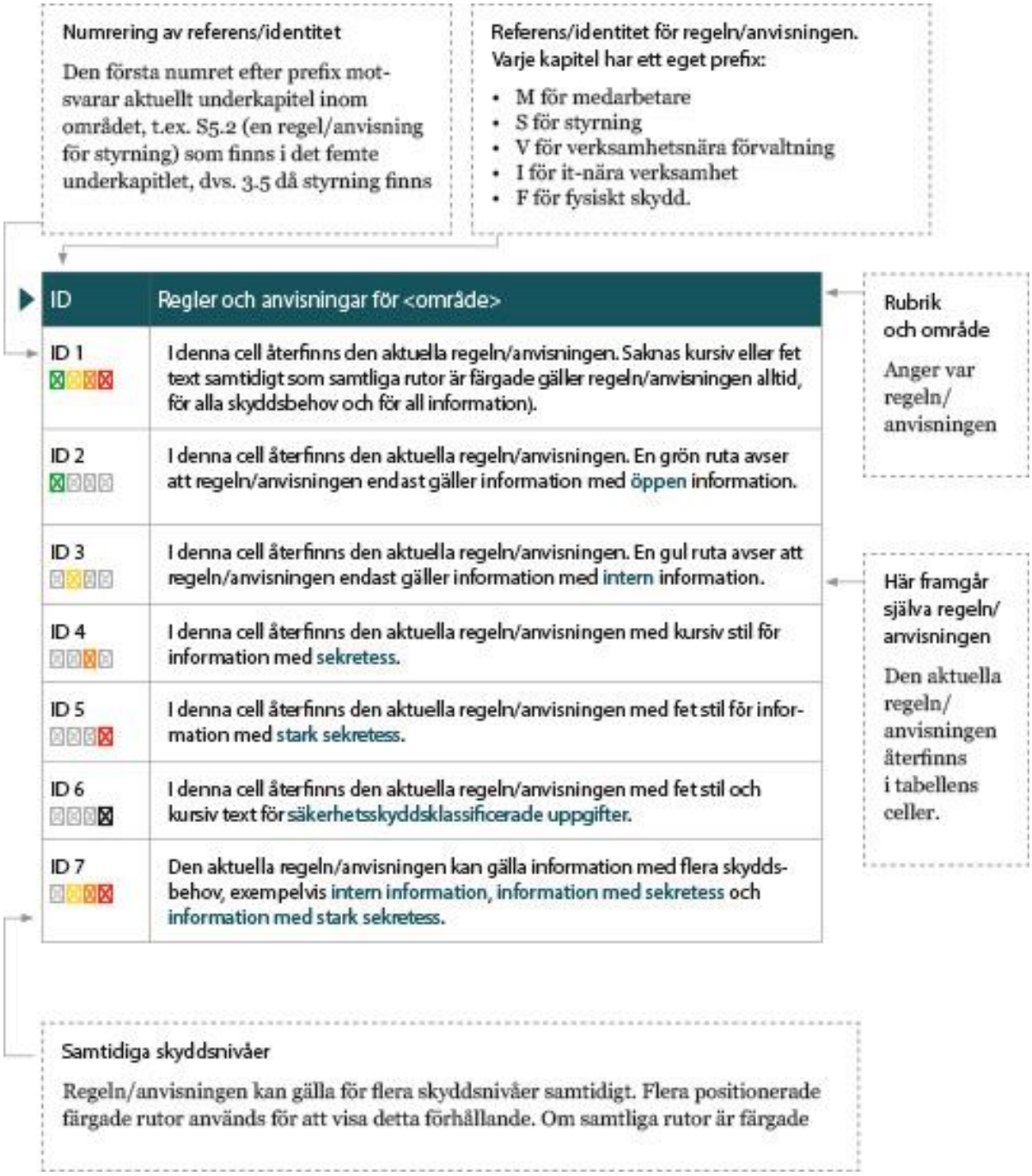


Bild förklaring: Bilden ovan förklarar uppbyggnaden av tabeller i handboken. kolumn ID innebär numrering av referens/identitet. Det första numret efter prefix motsvarar aktuellt underkapitel inom området. M står för medarbetare, S för Styrning, V för verksamhetsnära förvaltning, I för IT-nära verksamhet och F för skydd. Efter ID kommer rubrik och område.

Positionerade färgade rutor visar hur regeln/anvisningen ska tillämpas:

0 Grön ruta avser information med informationsklass 0 för konfidentialitet (öppen information).

1 Gul ruta avser information med informationsklass 1 för konfidentialitet (intern information).

2 Orange ruta avser information med informationsklass 2 för konfidentialitet (information med sekretess).

3 Röd ruta avser information med informationsklass 3 för konfidentialitet (information med stark sekretess).

4 Svart ruta avser information med informationsklass 4 för konfidentialitet (Säkerhets-skyddsklassificerad information) – samma position som röd ruta.

Grå ruta avser ett tomt fält.

Läsbarheten ökas genom att text skrivs med:

- *kursiv* stil för information med sekretess
- **fet stil** för information med stark sekretess
- ***fet stil*** och kursiv text för säkerhets-skyddsklassificerad information.

Nedan finns ett exempel från kapitel 2 – Informationssäkerhet för medarbetare om regler och anvisningar för fysisk hantering av mobila enheter.

ID	Regler och anvisningar för fysisk hantering av mobila enheter
M 6.7 0 1 2 3	Iaktta försiktighet när du arbetar i publika miljöer. Skydda helst skärmen med insynsskydd.
M 6.8 0 1 2 3	Undvik arbete med information med sekretess i publika miljöer. Om det är nödvändigt ska du arbeta avskilt så att informationen inte röjs för obehöriga.
M 6.9 0 1 2 3	Undvik arbete med information med stark sekretess i -publika miljöer helt. Om det i undantagsfall är nödvändigt måste du vidta åtgärder (t.ex. insynsskydd på mobil enhet) och arbeta avskilt så att informationen inte röjs för obehöriga.

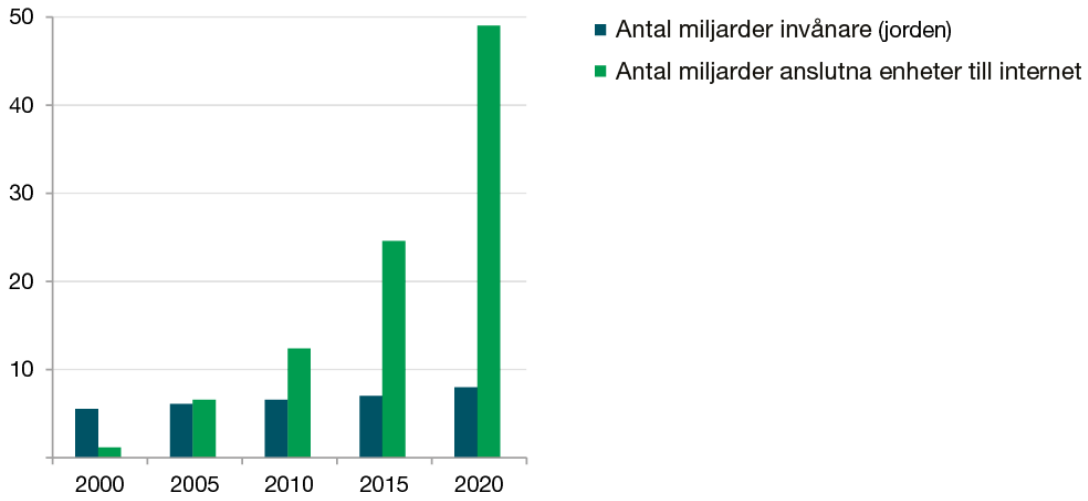
Tabell. 2 Exempel på regler och anvisningar ur handboken.

1.5 Samhällets digitalisering

Sverige befinner sig i en samhällsutveckling som benämns digitalisering. I princip alla delar av samhället – privatpersoner, företag, myndigheter och organisationer – använder datorer inom de flesta områden och till allt fler tjänster. Datorerna är i sin tur uppkopplade till ett gemensamt nätverk: internet.

Möjligheterna med digitaliseringen är enorma och den allt mer utbredda användningen av internet skapar helt nya möjligheter att utföra tjänster och dela information. Privatpersoner kan utföra en mängd digitala tjänster via internet (e-tjänster) – bankärenden, inköp, deklaration, bokningar, omröstning osv. – och denna utveckling har lett till att de flesta i dag förväntar sig att även kommunen ska erbjuda digitala tjänster via internet.

Men det är inte bara traditionella datorer som är uppkopplade mot internet. Även miljontals andra saker – allt från kameror till bilar – blir allt eftersom uppkopplade mot internet (s.k. internet of things – IoT). Digitaliseringen ses som en möjliggörare och motor för en utveckling som ger helt nya förutsättningar för samhället och människan. Hur det ser ut om 20 år är svårt att föreställa sig och omöjligt att veta; i dag går utvecklingen mycket snabbt mot något som samhället bara sett början på.



Figur 3. Utveckling av antalet anslutna enheter till internet. Figuren visar utvecklingen av antalet anslutna enheter per antal miljarder invånare på jorden. Detta från åren 200-2020 med fem års intervall. År 2000 fanns det 1 miljard anslutna enheter på 5 miljarder människor, 2020 fanns det närmare 50 miljarder enheter på ca 8 miljarder människor.

Säkert är att digitaliseringen innebär stora förändringar för kommunal verksamhet inom de flesta områden. Nya företeelser som e-hälsa, e-förvaltning, e-demokrati, intelligenta transportsystem och smarta städer införs löpande, och digitalisering är redan mycket mer och samhällsomfattande än bara kommuners it-drift.

Denna utveckling kommer att förändra mycket i grunden: vad vi gör, hur vi gör det och vad som går att göra. Information kommer att flöda i allt större mängder genom och mellan organisationer samt till och från privatpersoner. Exempelvis kommer kommunens information att tillgängliggöras i högre grad genom individuellt anpassade digitala tjänster. Service och förvaltningar kommer att göras mer transparenta och medborgare kommer i högre grad att kunna kommunicera med beslutsfattare.

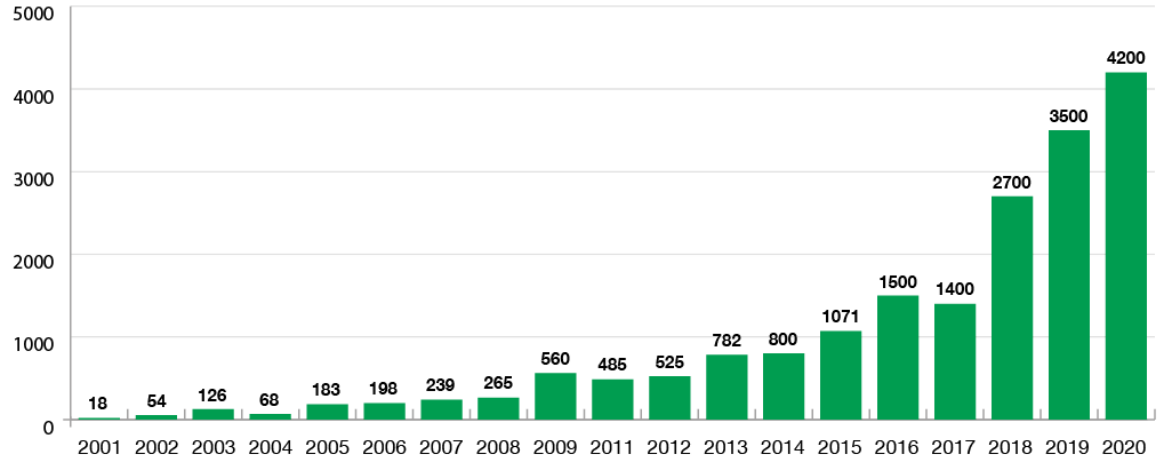
1.6 Digitaliseringens utmaningar och hot

Men parallellt med digitaliseringens möjligheter finns också utmaningar och hot. Information är inte längre enbart en organisations tillgång och angelägenhet utan den flödar mellan organisationer i näringsliv och offentlig förvaltning samt till och mellan enskilda och över nationsgränser. Gränser blir otydliga mellan vem som äger och vem som ansvarar för viss information, vilket gör det svårare att definiera hur den får användas, vem som kan och får ändra informationen, var ursprungsinformationen finns osv.

I och med att internet är en arena för hela samhället är det också en plats för samhällets baksidor. Virus, skadlig kod, falska nyheter, bedrägerier, identitetskapningar, utpressning, stölder, näthat och förföljelse är företeelser som finns i olika former på internet. Organiserad kriminalitet, extrema aktivistgrupper, terroristgrupper och odemokratiska stater har för länge sedan flyttat delar av sin verksamhet till internet. I dag behöver man inte vara it-expert för att

utföra destruktiva handlingar på nätet, utan skadliga tjänster kan köpas på välorganiserade marknadsplatser där handel sker anonymt och krypterat.

Hela tiden sker mängder av informationsrelaterade incidenter i Sverige och internationellt, vilka beror såväl på avsiktliga attacker som på misstag och olyckor. Introduktion av nya tillämpningar i framtiden kommer att erbjuda enorma tekniska möjligheter men även skapa nya typer av hot, t.ex. otillåten påverkan av artificiell intelligens i självkörande fordon. Denna utveckling innebär sammantaget stora utmaningar för kommunens informationssäkerhet.



Figur 4. Kostnader för skador relaterade till cyberbrottslighet rapporterade till IC3 (exklusive 2010) i miljoner USD. Bilden visar en graf som sträcker sig från 2001-2020, som visar på en gradvis ökning från 18 incidenter 2001 till 4200 incidenter 2020.

1.7 Informationssäkerhet, lagar och regleringar

Samhällets utveckling och digitalisering har också drivit lagstiftning och andra regleringar inom området framåt de senaste decennierna. Några av de viktigaste externa krav som reglerar en kommuns arbete inom informationssäkerhetsområdet är

- dataskyddsförordningen (GDPR)
- offentlighets- och sekretesslagen
- säkerhetsskyddslagen
- lag om informationssäkerhet för samhällsviktiga och digitala tjänster
- regleringar inom civilt försvar och krisberedskap.

I Sverige är Myndigheten för samhällsskydd och beredskap, MSB, samordnande på nationell nivå för frågor som rör informationssäkerhet, och myndigheten tillhandahåller information om informationssäkerhet för det offentliga Sverige. I kapitel 7.2.4 – Lagar och regelverk som relaterar till informationssäkerhet finns en lista och sammanfattande beskrivning över vilka lagar och förordningar som innehåller de regleringar av informationssäkerhet som gäller för verksamheter i Sverige.

1.8 Varför är informationssäkerhet viktigt?

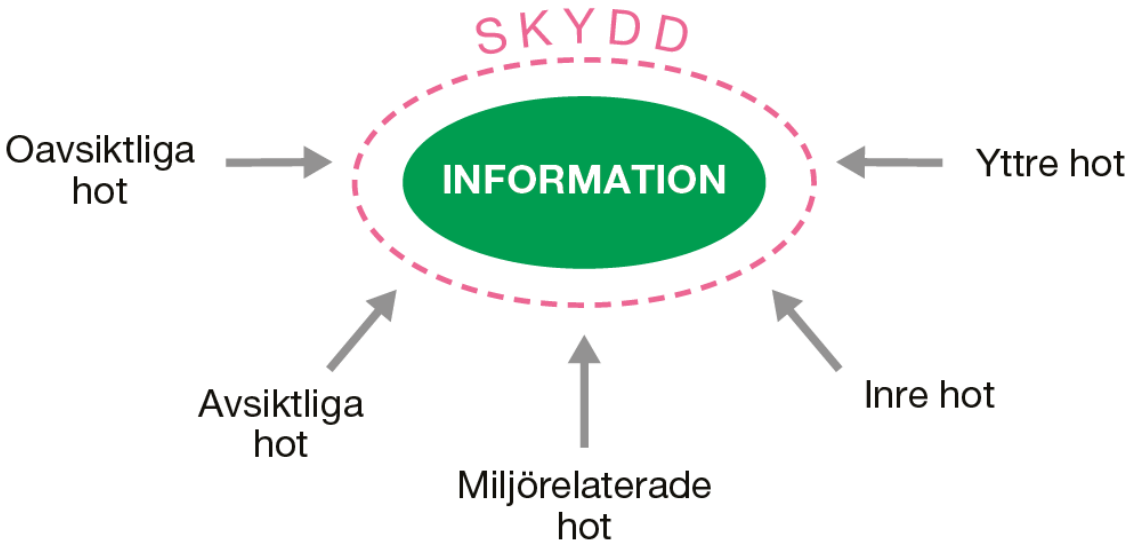
Information är en strategisk resurs för Linköpings kommun. Utan den kan vi inte bedriva vår verksamhet. Vi behöver därför informationssäkerhet för att uppfylla våra åtaganden gentemot både allmänhet och medarbetare. Informationssäkerhet är också en förutsättning för att vi ska kunna skapa en tillförlitlig e-förvaltning med nya digitala tjänster och därmed kunna delta i det digitala samhället.

Därför behövs informationssäkerhet
Informationssäkerhet är kommunens förmåga att hantera informationen så att legala, etiska, och verksamhetsmässiga intentioner upprätthålls. Målsättningen med kommunens informationssäkerhetsarbete är därför att skydda kommunen, dess verksamhet och invånare som annars riskerar att skadas genom bristande informationssäkerhet.

1.9 Introduktion till informationssäkerhet

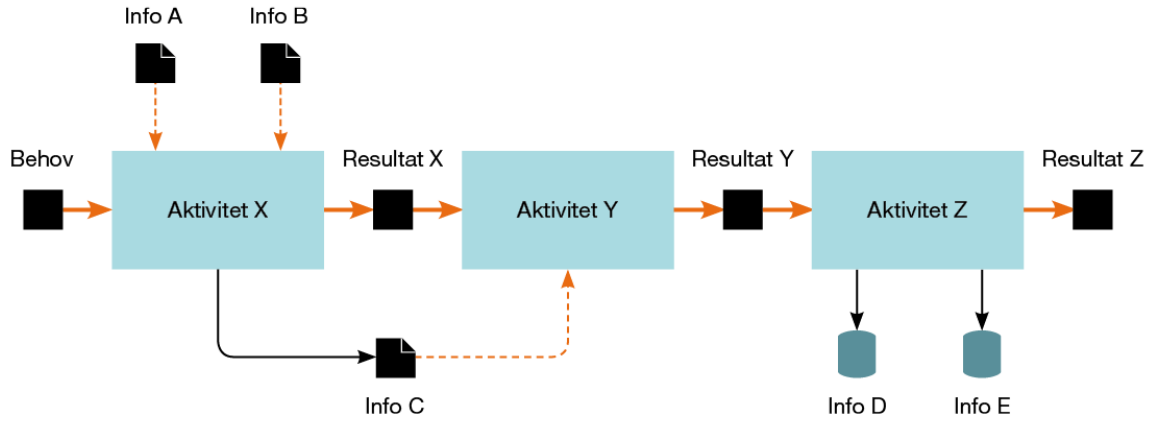
Informationssäkerhet handlar om att skapa och upprätthålla ett lämpligt skydd av information. Information behöver försvaras mot de hot den utsätts för. Det gäller information i alla dess former – text, ljud, bild, film osv. – och oavsett hur den lagras, bearbetas och kommuniceras.

Informationen kan dessutom hanteras med stöd av it, på papper eller direkt av människor i form av tal. Medan It-säkerhet fokuserar på säkerhet i datorer och datornätverk handlar informationssäkerhet om all information oavsett form – alltså även pappersbaserad information samt information som finns i människors huvuden.



Figur 5. Information behöver skyddas mot omkringliggande hot. Figuren ovan visar hur ordet “information” är inringat av en skyddscirkel. Denna cirkel skyddar mot olika typer av omkringliggande hot. Så som oavsikltiga hot, avsiktliga hot, yttre hot, miljörelaterade hot och inre hot, som försöker tränga sig in i skyddcirkeln.

En del av vår information är värdefull (betydelsefull, viktig) både för den verksamhet vi bedriver och för den enskilda individen – allt från lönelistor och elevbetyg till mötesprotokoll eller information om banktillgångar. Ibland är informationen livsviktig eller kritisk såsom i patientjournaler eller i de it-system som styr kommunens dricksvattenförsörjning. Om vi inte kommer åt denna information när vi behöver den, eller om det är fel i den, kan det få katastrofala följder. Den information som värdefull för vår verksamhet benämns inom informationssäkerhet som skyddsvärd information. I våra verksamheter flödar information i alla dess former. Information inhämtas och bearbetas och ny information skapas. Detta sker i alla verksamheters olika processer. Informationen som skapas i processer förekommer i flera olika former, exempelvis pappersbunden, digital eller muntlig information.



Figur 6. Information inhämtas och skapas i verksamhetens olika processer. Bilden beskriver hur ett förlopp där ett behov går igenom flertalet aktiviteter, som tillsammans med olika typer av information, genererar ett resultat.

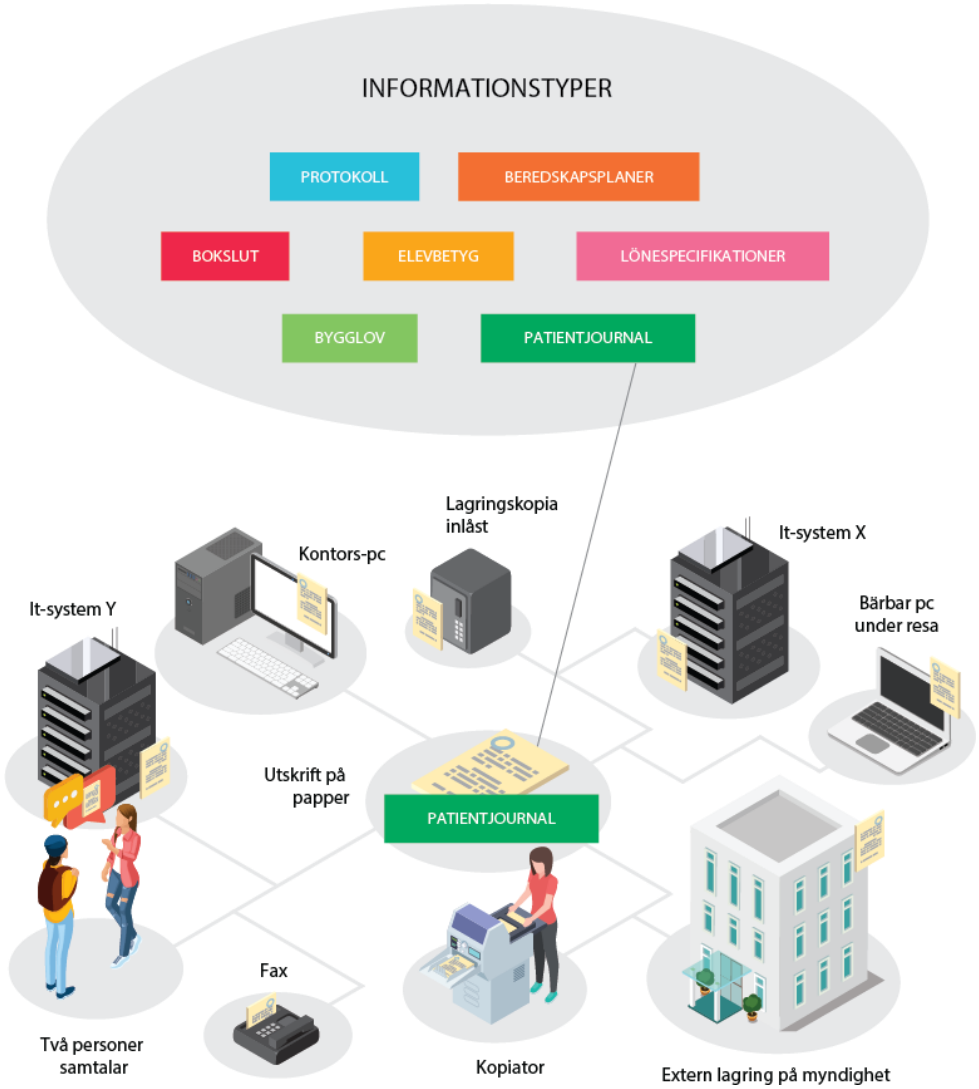
1.10 Grundläggande principer och begrepp

När information definieras i ett säkerhetsarbete handlar det vanligen om information som en viss mängd eller en viss typ av information. Denna mängd eller typ benämns informationstillgång, informationsmängd eller informationstyp och kan bestå av t.ex. patientjournaler, elevakter, bokslut eller beredskapsplaner. Vidare i handboken kommer vi främst använda begreppet informationstyp. De resurser (datorer, pappersark, människor etc.) som används för att hantera informationstillgången* benämns informationsbehandlingsresurser. Vanliga benämningar på dessa resurser är informationsbärare/bärare eller informationsresurser/resurser.

I handboken kommer vi främst använda begreppen bärare eller resurser. Även begreppet utrustning kommer att användas, eftersom utrustning ofta är bärare av information. När vi diskuterar informationster i handboken förutsätter vi i ett brett perspektiv att dessa typer har ett värde yp (är betydelsefulla) för verksamheten.

* I vissa definitioner inkluderar begreppet informationstillgång både själva informationen och informationshanterande resurser, t.ex. manuella och it-baserade informationssystem. I handboken avses dock den information som bedöms som värdefull för verksamheten.

Hos de flesta organisationer är informationstyperna vanligen spridda i hela verksamheten och återfinns i många olika informationsbärare. I figur 7 nedan har informationstillgången till en patientjournal exemplifierats för att tydliggöra detta. Denna informationstyp finns i många olika bärare och i många former – allt från elektronisk form i olika resurser som it-system och datorer till pappersform och muntlig form. För en organisation är informationstypen vital och behöver skyddas för att verksamhet eller individer inte ska skadas. När vi skapar skydd för informationstyper i vårt informationssäkerhetsarbete är det viktigt att beakta alla dessa perspektiv när vi hanterar, bearbetar och lagrar informationen.



Figur 7. En informationstyp återfinns vanligen i flera olika bärare. Bilden visar flertalet informationsbärare såsom kopiatorer, fax, personer som samtalar, bärbar PC samt kontors-pc. Dessa bärare är sammankopplade till en patientjournal, som påvisar flertalet vanligen spridda informationstyper, så som protokoll, bokslut, journaler, bygglov etc.

1.11 Så här skyddar vi informationstyper

För att skydda informationstyperna i kommunen behöver vi säkerhetsställa att de fyra aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet tillgodoses. I allt informationssäkerhetsarbete är dessa fyra informationssäkerhetsaspekter den utgångspunkt från vilken vi initierar sökandet efter lämpligt skydd.

- Konfidentialitet - Att information inte tillgängliggörs eller avslöjas till obehörig.
- Tillgänglighet -Att information är åtkomlig och användbar av behörig
- Spårbarhet- Att förändring i information går att spåra och återskapa
- Riktighet- Att infromation är korrekt, aktuell och fulständig

figur 8. Informationssäkerhetens fyra aspekter. Figuren är beskriven i texten ovan.

Ofta finns krav kopplade till våra informationstyper, vilka kan relateras till de fyra aspekterna. Dessa krav kan vara våra egna (interna krav), ibland härledas till omvärlden (externa krav, t.ex. lagkrav, avtal eller standarder) eller bestå av förväntningar och behov hos externa aktörer. Ett typiskt internt krav kan vara att en informationstyp alltid ska vara tillgänglig (tillgänglighet) under kontorstid. Ett vanligt externt krav kan vara att en specifik informations-typ inte får läsas (konfidentialitet) av någon obehörig (någon som inte har behörighet). Vanliga externa krav finns ofta formulerade i olika avtalsrelationer mellan kommunen och andra individer eller organisationer.

Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering, vilket ofta inbegriper krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Dessutom har externa aktörer normalt sett behov och förväntningar som påverkar vår informationssäkerhet.

Vilken omfattning av och kvalitet på skyddet (skyddsnivå) som är lämplig för en viss informationstyp beror på konsekvenser för verksamheten eller individer om informationen

- avslöjas till obehörig (röjs)
- inte är korrekt eller aktuell
- inte finns tillgänglig när den behövs, eller
- inte går att spåra eller återskapa.

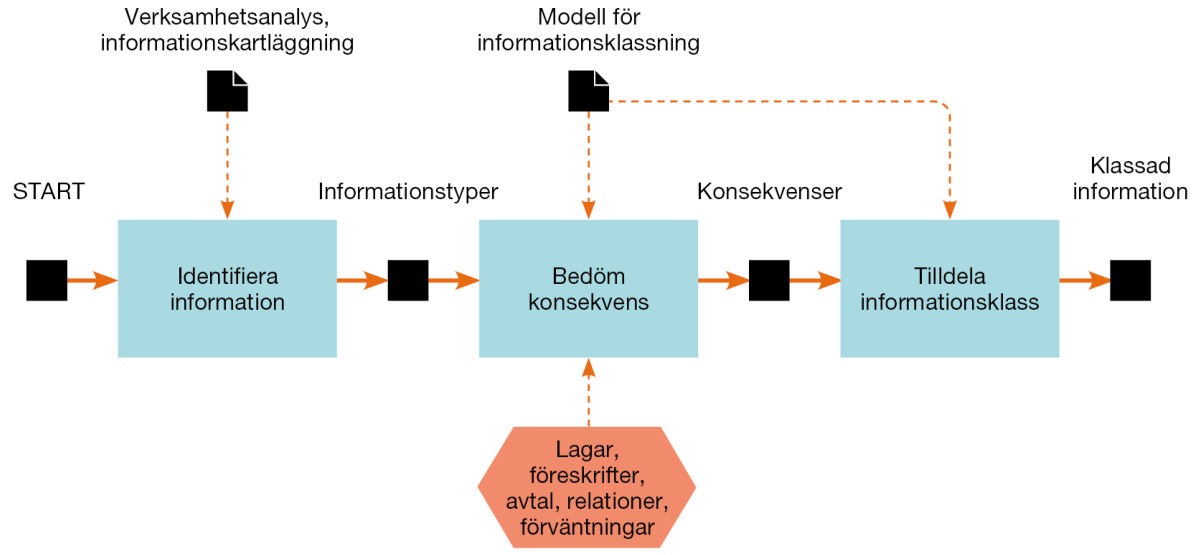
Lämplig skyddsnivå kan även avgöras genom en analys av aktuell hotbild och i vilka situationer informationen hanteras, dvs. hur den lagras, bearbetas, kommuniceras osv.

1.12 Grunderna i informationsklassning

Den process som används i arbetet med informationssäkerhet för att klarlägga skyddsbehov för informationstyper kallas informationsklassning.

Informationsklassning enligt standarden ISO/IEC 27002 Mål: att säkerställa att information får en lämplig skyddsnivå i enlighet med dess betydelse för organisationen.

En informationsklassning genomförs som en process uppdelad i tre aktiviteter. Nedanstående figur 10 visar dessa aktiviteter övergripande.



Figur 9, Aktiviteter vid informationsklassning. Figuren visar en övergripande informationsklassningprocess. Där man börjar med aktviteten att “Identifiera information med hjälp av verksamhetsanalyser och informationskartläggning. Denna aktivitet förs sedan vidare som informationstyper till nästa aktivitet, “Bedöm konsekvenser”. som med hjälp av input från en modell för informationsklassning, lagar, avtal och föreskrifter producerar konsekvenser som förs vidare till

den tredje aktiviteten. “Tilldela informationsklass”, där man tilldelar en informationsklass och sedan skapar klassad information.

- Identifiera information
  Denna aktivitet kan utföras på olika sätt och varierar från organisation till organisation. Här kartläggs informationshanteringen och informationstyper identifieras.
- Bedöm konsekvens för verksamheten
  Denna aktivitet analyserar vilka konsekvenser en informationsskada orsakar för verksamheten. Här används den modell som beslutats för informationsklassning tillsammans med krav och förväntningar relaterade till informationen. Observera att bedömningen upprepas för samtliga fyra informationssäkerhetsaspekter.
- Tilldela informationsklass
  Konsekvensen för verksamheten styr i vilken informationsklass informationen placeras: ju allvarligare konsekvens – desto högre informationsklass. Informationsklassen uttrycker ett skyddsbehov som relaterar till en skyddsnivå som i sin tur beskriver hur verksamheten behöver skydda informationen. Den färdiga informationsklassningen för informationen består alltså av fyra värden: ett värde för konfidentialiet, ett för riktighet, ett för tillgänglighet samt ett för spårbarhet.

Linköpings kommuns modell för informationsklassning beskrivs i kapitel 3 – Styrning av informationssäkerhet. Regler och anvisningar för hur information ska skyddas utifrån kommunens modell återfinns i framför allt kapitel 2 – Informationssäkerhet för medarbetare, kapitel 5 – Informationssäkerhet i it-nära förvaltning och kapitel 6 – Infomationssäkerhet och fysiskt skydd.

1.13 Skyddsåtgärder

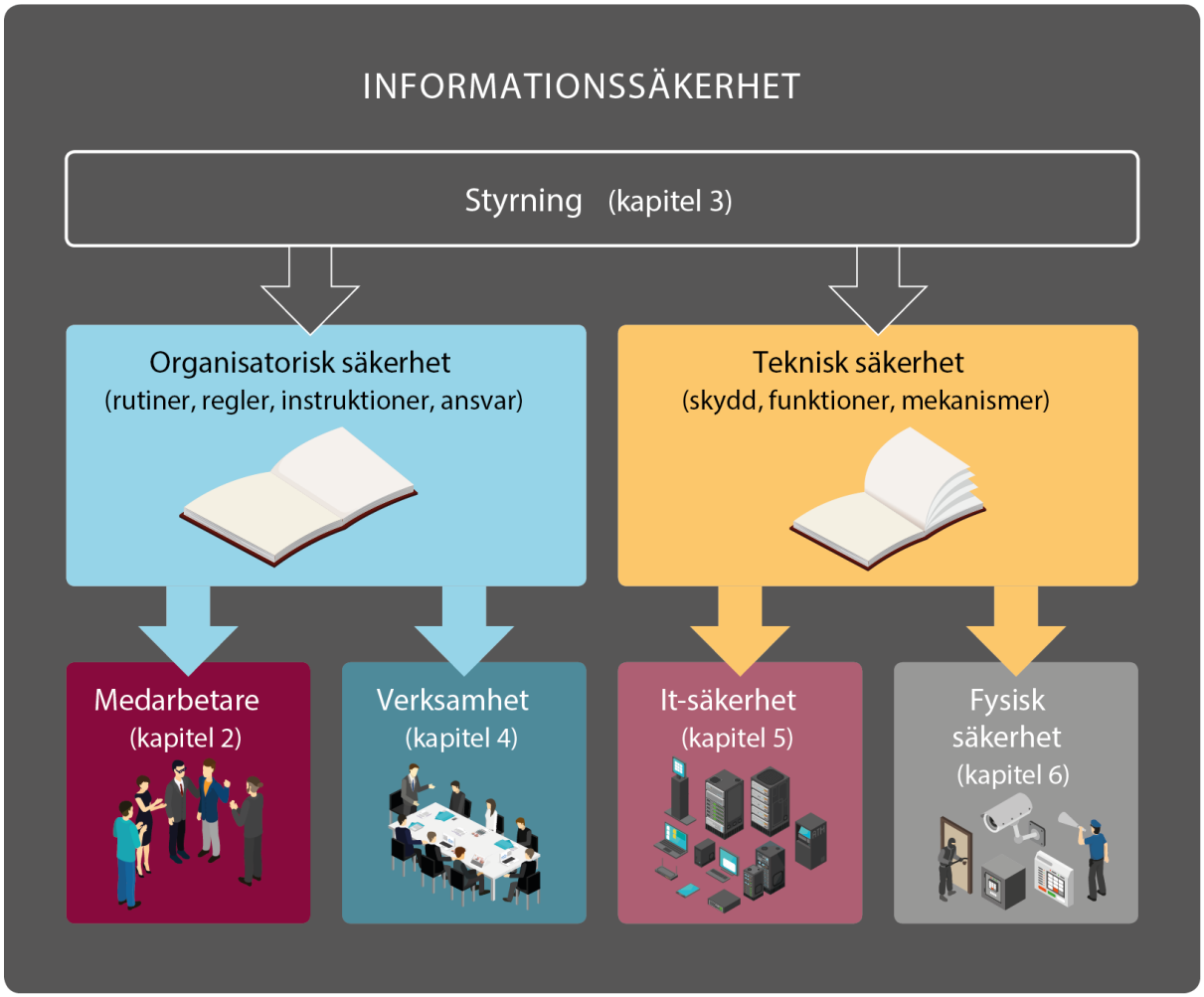
De åtgärder som behöver vidtas för att möta krav och förväntningar på vår verksamhet brukar vanligen benämnas skyddsåtgärder.

Skyddsåtgärder tillhör något av två huvudområden inom informationssäkerhet: organisatorisk säkerhet respektive teknisk säkerhet. De tekniska huvudområdet delas sedan i sin tur upp i it-säkerhet och fysisk säkerhet.

Organisatoriska skyddsåtgärder omfattar införandet och förvaltningen av regelverk via policyer, riktlinjer, rutiner, regler och instruktioner och anknyter nästan alltid till mänskligt agerande och beteende. Skyddsåtgärder inom den organisatoriska säkerheten är ofta knutna till organisation, verksamhet och styrning. Åtgärderna handlar till stor del om att få medarbetare och verksamhet att ta ansvar, arbeta strukturerat och agera korrekt. All styrning av informationssäkerhet i en verksamhet har sitt ursprung i det organisatoriska informationssäkerhetsområdet.

Figur 10. Organisatorisk säkerhet styr och driver fysisk säkerhet och it-säkerhet. Figuren visar tre horisontella pilar liggandes bredvid varandra. Första och översta pilen är döpt till “IT-säkerhet”. Andra och mellersta pilen som är större till utformningen är döpt till “organisatorisk säkerhet”. Tredje och sista pilen är döpt till “fysisk säkerhet”.

Tekniska skyddsåtgärder består av faktiska fysiska skydd, funktioner eller mekanismer. De tekniska skyddsåtgärderna utgörs oftast av en enhet, en programvara, ett säkerhetsskåp eller en lokal av en viss typ. Brandväggar, kryptering och säkerhetskopiering är exempel på tekniska it-säkerhetsskydd medan skal-, inbrotts- och brandskydd är exempel på fysiska skydd. Inom den tekniska säkerheten handlar det främst om att anpassa skyddens omfattning, egenskaper och kvalitet så att krav och förväntningar uppfylls.



Figur 11. Skyddsåtgärdernas indelning inom informationssäkerhet, kapitel i handboken. Följande text nedan beskriver bildens innehåll.

Den organisatoriska säkerheten i kommunen behandlas i kapitel 2–4 och den tekniska säkerheten behandlas i kapitel 5–6.

Oftast märker medarbetaren i en verksamhet inte av skyddsåtgärderna; det gäller framför allt de tekniska skydden. De organisatoriska skyddsåtgärderna berör generellt sett fler och märks sannolikt mer i det dagliga arbetet.

1.14 Riskhantering och informationssäkerhet

Begreppet risk används inom informationssäkerhetsarbetet. En risk mäts utifrån sannolikheten att en incident inträffar och konsekvensen av denna incident. Kartläggning av informationssäkerhetsrelaterade risker för information, verksamheter och informationsbärare hanteras inom området riskhantering och utgör en central del i allt arbete med informationssäkerhet. I kapitel 3 – Styrning av informationssäkerhet återfinns mer information om hur kommunen arbetar med risker inom informationssäkerhetsområdet.

1.15 Ledningssystem för informationssäkerhet (LIS)

Ett ledningssystem för informationssäkerhet (förkortat LIS) är den del av en verksamhets totala ledningssystem som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, t.ex. planering och uppföljning. Kommunens systematiska informationssäkerhetsarbete bygger på standarder i ISO/IEC 27000-serien. Märk att ISO/IEC 27000-serien kallar skyddsåtgärder för säkerhetsåtgärder.

- SS-ISO/IEC 27001 Informationsteknik – Säkerhetstekniker -Ledningssystem för informationssäkerhet – krav. Denna standard ställer krav på vad ett LIS ska innefatta. I standardens bilaga A finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas.
- SS-ISO/IEC 27002 Informationsteknik – Säkerhetstekniker ----– Riktlinjer för informationssäkerhetsåtgärder. Denna standard ger vägledning för hur säkerhetsåtgärderna i föregående standards bilaga A kan införas.

Dessa båda standarder är de dominerande ramverken för att styra arbetet med informationssäkerhet, både i Sverige och internationellt.

Standarderna utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet arbete. Historiskt har området informationssäkerhet varit teknikdrivet med fokus på insatser för att säkra den tekniska utrustningen (bäraren). Liten hänsyn har tagits till vilken information utrustningen hanterar. Utgångspunkten i 27000-serien är att det är just informationen som ska skyddas utifrån konfidentialitet, riktighet, tillgänglighet och spårbarhet, medan alla resurser (utrustningen) som hanterar informationen är sekundära.
Att standarden är så etablerad och spridd innebär en rad fördelar. Förutom att den tar tillvara kunskaper och erfarenheter globalt innebär den också ett gemensamt ramverk och en gemensam terminologi som underlättar kommunikation och samverkan med andra aktörer vid exempelvis utbildning, revision och upphandling.

Ledningssystemet bygger på verksamhetens planerings- och uppföljningscykler. Dessa cykler innebär t.ex. att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och verksamhetskontroller samt regelbundet ser över styrdokument. Nedanstående figur 12 visar dessa planerings- och uppföljningscykler tillsammans med stödjande processer och moment.

Figur 12. Ledningssystem för informationssäkerhet (LIS). Källa: MSB. Figuren visar dessa LIS-planerings- och uppföljningscykler i form utav ett inner hjul med 4 kategorier med tillhörande uppföljningscykler i form utav kugghjul.

1. Identifiera och analyser, tillhörande kugghul är verksamhet, “omvärld”, “ GAP” och “risk”.
2. Utforma, tillhörande kugghjul är “Roller och ansvar”, “Mål”, “styrdokument”, handlingsplan och klassning.
3. Använda, tillhörande kugghul är “Genomföra och efterleva”, “klassa information”, “utbilda och kommunicera”, “granska” och “övervaka”
4. Följa upp och förbättra, tillhörande kugghul är ”uppfylla mål”, “utvärdera” och “Ledningens genomgång”.

Kapitel 2 - Informationssäkerhet för medarbetare

2.1 Inledning

I detta kapitel finns de regler och anvisningar som ska följas av dels medarbetare inom Linköpings kommun, dels medarbetare hos externa aktörer[1], t.ex. inhyrda konsulter, entreprenörer, organisationer samt förtroendevalda och andra som på olika sätt hanterar kommunens information. När begreppet medarbetare används i texten gäller det samtliga ovanstående roller.

Observera att begreppet medarbetare även inkluderar förtroendevalda samt personer från externa aktörer eftersom även dessa hanterar kommunens information.

Kapitlet beskriver även det ansvar som medarbetarna har i förhållande till de regler och anvisningar som finns om hur information ska hanteras. Reglerna och anvisningarna i denna handbok ersätter dock inte lagar, förordningar och föreskrifter, utan det är ditt ansvar som medarbetare att följa handboken tillsammans med rättsliga krav.

Reglerna och anvisningarna i detta kapitel gäller däremot inte elever vid kommunens skolor eller brukare vid kommunala boenden som använder informationsresurser (t.ex. datorer, kopiatorer eller telefoner) som är kopplade till Linköpings kommuns nät men där personerna inte hanterar kommunens information. För dessa användare ska det finnas separata regelverk som hanteras av respektive verksamhet. Fråga din närmaste chef[2] om råd i förekommande fall. Även informationssäkerhetssamordnaren kan vara ett stöd när ett sådant regelverk tas fram.

Utbildning och information inom informationssäkerhet sker årligen och systematiskt i linjeverksamheten.

[1] Personer från dessa verksamheter kan också betecknas uppdragstagare. För att någon ska anses vara uppdragstagare
i offentlighets- och sekretesslagens mening krävs att uppdraget ges direkt till en fysisk person. Uppdragstagaren har inte rätt att sätta någon annan i sitt ställe. Uppdragstagaren är normalt så knuten till myndigheten att hen kan sägas delta i myndighetens egentliga verksamhet, dvs. som regel myndighetens uppgifter enligt instruktion eller motsvarande reglering.

[2] Externa aktörer som exempelvis konsulter söker i första hand råd hos respektive uppdragsgivare. Förtroendevalda söker råd hos kommunens informationssäkerhetssamordnare.

Vem äger informationen?
Tänk på att kommunen i de flesta fall äger all information som behandlas i kommunens datorer, telefoner, e-postlådor, molntjänster, dokument etc. och har när som helst möjlighet att granska innehållet enligt gällande regler och lagar.

2.2 Samtliga medarbetare ansvarar för informationssäkerheten

Kommunen hanterar dagligen stora mängder information inom olika verksamheter och områden, t.ex. utbildning, socialtjänst, stadsplanering och -bygglov. Information förekommer i olika former – muntlig, skriftlig samt i olika it--system – och den finns främst i form av text men även som bilder, symboler, filmer och ljud.

Kommunen har ett ansvar att skydda informationen från att obehöriga tar del av den. Det kan exempelvis gälla information som på något sätt relaterar till enskilda- individers personliga integritet, där dessa individer riskerar att lida skada om informationen röjs. För att skydda information finns det lagstiftning som kommunen är skyldig att efterleva, såsom offentlighets- och sekretesslagstiftning samt dataskyddslagstiftning. Utöver detta finns en förväntan på att kommunen hanterar informationen på ett korrekt och säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla ett skydd för att uppfylla såväl lagstadgade krav som, i den mån det är rimligt, medborgares och andra aktörers förväntningar på kommunen.

Information behöver skyddas på olika sätt. Skyddet kan vara tekniskt, exempelvis- via en brandvägg i ett it-nätverk, eller organisatoriskt i form av regler, t.ex. de regler och anvisningar som presenteras här. Ett skydd kan också vara fysiskt och skydda information genom låsta utrymmen eller inbrottsklassade skåp.

Ett av de mest effektiva skydden mot oönskade händelser är att du som med-arbetare är medveten om värdet på den information du hanterar och har goda kunskaper om hur den ska hanteras. En god säkerhetskultur i kommunen skapas genom engagerade och motiverade medarbetare som förstår att alla bidrar till helheten. En stor del av kommunens informationssäkerhet beror därför på hur varje medarbetare hanterar informationen.

Du som medarbetare måste följa kommunens tillämpningsanvisningar för informations-säkerhet. Det är kommunens chefer som har att säkerställa att samtliga medarbetare får adekvat utbildning i informationssäkerhet. Om dessa tillämpningsanvisningar för informationssäkerhet inte efterlevs kan kommunens rutiner för disciplinärenden komma att tillämpas.

Tänk på att när du skapar, förändrar eller förädlar information i ditt arbete så -behandlar du vanligtvis information som är kommunens. Du är därför alltid -skyldig att följa de tillämpningsanvisningar som gäller för behandling av kommunens information, oavsett situation.

2.2.1 Yttrandefrihet

Yttrandefriheten är en grundlagsskyddad rättighet som innebär att alla medborgare har rätt att i tal skrift eller bild fritt uttrycka sina åsikter om offentliga verksamheter, t.ex. en kommun. Som offentligt anställd får du därför i stor utsträckning säga vad du tycker. Yttrandefriheten kan dock vara begränsad genom lag eller annan författning, oftast offentlighets- och sekretesslagen.

Yttrandefriheten för offentligt anställda skyddas genom att arbetsgivaren är skyldig att respektera den och inte får vidta åtgärder som har karaktär av bestraffning eller något slags sanktion mot en anställd för att hen har nyttjat sin rätt att yttra sig.

2.2.2 Meddelarfrihet

Du som är offentligt anställd har rätt att informera medierna om i stort sett vad som helst (med undantag av vissa uppgifter som framgår av offentlighets- och sekretesslagen). Detta benämns meddelarfrihet, vilket innebär en rätt att lämna ut uppgifter, bl.a. ur allmänna handlingar. Meddelarfriheten innebär inte att du har rätt att lämna ut sekretessbelagda handlingar.

När du använder din meddelarfrihet är du också skyddad från att arbetsgivaren gör efterforskningar om vem som informerat media. Med andra ord får inte en chef eller överordnad fråga vem som sagt något, vad som blev sagt eller ens till vem det sades.

Regler och anvisningar i handboken påverkar inte din grundlagsskyddade yttrandefrihet eller din meddelarfrihet som offentligt anställd.

ID	Regler och anvisningar för medarbetare och uppdragstagare
M 2.1 	Du ska hantera kommunens information enligt kommunens regler och anvisningar.
M 2.2 	Det är inte tillåtet att lagra eller bearbeta kommunens information i annan utrustning (dator, mobil etc.) eller i it-tjänster (it-system, moln-tjänster, mobilappar etc.) än de som kommunen tillhandahåller eller har avtalat om.
M 2.3 	Du ska följa lagar och andra regelverk som gäller dig i din tjänste-utövning. När du har informerats om detta kan arbetsgivaren begära att du ska skriva under att du tagit del av information.
M 2.4 	Du är skyldig att skyndsamt anmäla incidenter och brister till närmaste-chef. Notera att för personuppgiftsincidenter gäller särskilda regler. Kommunen måste anmäla personuppgiftsincidenter till Integritets-skyddsmyndigheten inom 72 timmar.

2.3 Informationsklasser för konfidentialitet

Oavsett vilken typ av verksamhet som bedrivs är viss information alltid mer skyddsvärd än annan. Därför skiljer sig skyddsbehovet åt mellan olika informationstyper och i olika situationer. Skyddsbehovet avseende konfidentialitet bedöms framförallt utifrån offentlighets- och sekretesslagstiftningen samt utifrån vilka konsekvenser det kan få för verksamheten eller för enskild om informationen röjs till obehöriga, i strid med dataskyddslagstiftningen. Kommunens modell för informationsklassning innehåller även informationssäkerhetsaspekterna riktighet, tillgänglighet och spårbarhet (se kapitel 3.7 – Informationsklassning i Linköpings kommun).

I kommunen finns fem informationsklasser för konfidentialitet (nivå 0–4) som tydliggör hur skyddsvärd informationen är för kommunen och hur den ska hanteras och får spridas:

- 0 Öppen
- 1 intern
- 2 Sekretess
- 3 Stark sekretess
- 4 Säkerhetsskyddsklassificerad

Varför klasser och vad betyder de?

Benämningarna av de fem informationsklasserna för konfidentialitet är valda för att ge kommunens medarbetare en indikation på vad som skiljer mellan klassningens olika skyddsnivåer. Med stigande skyddsnivå minskar antalet behöriga personer. På nivå 0 (öppen) kan informationen tillgängliggöras för alla inklusive allmänheten, medan på nivå 4 (säkerhetsskyddsklassificerade uppgifter) har ytterst få personer (av kommunens medarbetare) behörighet att hantera informationen. Den spridning informationen får ha kan alltså kopplas till informationens skyddsnivå; låg skyddsnivå tillåter större spridning än hög skyddsnivå.

I handboken används grafiska markeringar (fet, respektive kursiv stil) för begreppen sekretess, stark sekretess och säkerhetsskydds-klassificerad. Informationsklasserna för konfidentialitet illustreras i tabell 3.

Skyddsnivå och informationsklass för konfidentialitet	Behörighet/spridning	Generella exempel
4. Svart: Säkerhetsskydds-klassificerad information Mycket högt skyddsbehov	Säkerhetsskydds-klassificerad Informationen får - endast vara tillgänglig för med--arbetare som har särskild behörighet och behov av att hantera informationen. Informationen får endast hanteras i särskilt till-delad IT-utrustning.	• Information som rör Sveriges säkerhet • Information som regleras av Säkerhetsskyddslagen
3. Röd: Information med Stark sekretess Högt skyddsbehov	Stark sekretess Informationen får endast spridas och vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen eller i vissa fall extern part som har rätt att ta del av informationen med stöd av OSL.	• Socialtjänstakt • Adressuppgifter personal • Patientjournaler • Arbetsmaterial • Riktlinjer, rutiner, instruktioner etc
2. Orange: Information med Sekretess Förhöjt skyddsbehov	Sekretess Information får endast vara tillgänglig för och spridas till medarbetare som har behov av uppgiften i sin tjänsteutövning eller i vissa fall extern part som har rätt att ta del av informationen med stöd av OSL.	• Personalscheman • Löneinformation • Arbetsmaterial • Riktlinjer, rutiner, instruktioner etc.
1. Gul: Intern information Grundläggande skyddsbehov	Information som enbart är avsedd att spridas till medarbetare inom Linköpings kommun och externa aktörer som behöver informationen	• Information på Linweb • Arbetsmaterial • Riktlinjer, rutiner, instruktioner etc.
0. Grön: Öppen information Inget skyddsbehov	Öppen information som avses att spridas fritt inom och utom Linköpings kommun	Pressmeddelanden Broschyrer Information på linkoping.se

Tabell 3. Kommunens fem informationsklasser för konfidentialitet.

Informationsruta

Hantering av Säkerhetsskyddsklassificerad information redovisas inte vidare.

Observera att tabellen ovan redovisar kommunens samtliga fem informationsklasser för konfidentialitet. Den högsta skyddsnivån (Säkerhetsskyddsklassificerad) med svart färg kommer inte redovisas vidare i handboken eftersom hanteringen av den informationen regleras i en separat tillämpningsanvisning för de som har rätt att hantera sådan information.

Olika regler och anvisningar gäller för information som tilldelats någon av de fem informationsklasserna för konfidentielitet avseende spridning och hantering.

ID	Regler och anvisningar för spridning av information
M 3.1 	**Öppen** information (informationsklass 0) är avsedd att spridas fritt inom och utom kommunen. Ibland krävs dock beslut för att öppen information ska publiceras, t.ex. på externa webbplatser som www.linkoping.se.
M 3.2 	**Intern** information (informationsklass 1) är enbart avsedd att spridas till medarbetare inom Linköpings kommun och till externa aktörer som behöver informationen.
M 3.3 	Information med **sekretess** (informationsklass 2) får endast vara tillgänglig för och spridas till medarbetare som har behov av uppgiften i sin tjänsteutövning eller i vissa fall extern part som har rätt att ta del av informationen med stöd av OSL. Externa aktörer ska vid behov underteckna en blankett för tystnadsplikt om deras tystnadsplikt inte framgår direkt av lag eller i avtal med kommunen.
M 3.4 	Information med ***stark sekretess*** (informationsklass 3) får endast -spridas och vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen eller i vissa fall extern part som har rätt att ta del av informationen med stöd av OSL. Den externa aktören måste normalt också underteckna blankett för tystnadsplikt innan information delges om inte deras tystnadsplikt framgår direkt av lag eller i avtal med kommunen.

När någon begärt ut information med stöd av offentlighetsprincipen ska en prövning ske enligt offentlighets- och sekretesslagen. Vid en sådan prövning saknar informationsklassningen betydelse. Om begärd information har en hög informationsklass för konfidentialitet kan informationen innehålla sekretess-belagd uppgift. Därutöver kan informationsklassningen och dataskyddsför-ordningen påverka hur informationen lämnas ut.

Ansvaret för att klassa information, dvs. bedöma hur en viss typ av information ska klassas, innehas av utpekade roller i kommunens verksamheter. Om du inte känner till eller hittar informationens klassning i IHP eller förteckning över arbetsmaterial bör du rådfråga närmaste chef. I kapitel 3 – Styrning av informationssäkerhet och kapitel 4 –

Informationssäkerhet i verksamhetsnära förvaltning kan du läsa mer om hur ansvaret är fördelat och hur ansvaret fungerar.

Informationsklassning är ett hjälpmedel
Informationsklassning är ett stöd till alla medarbetare i kommunen för att hantera information på ett sådant sätt att kommunens negativa konsekvenser minimeras.

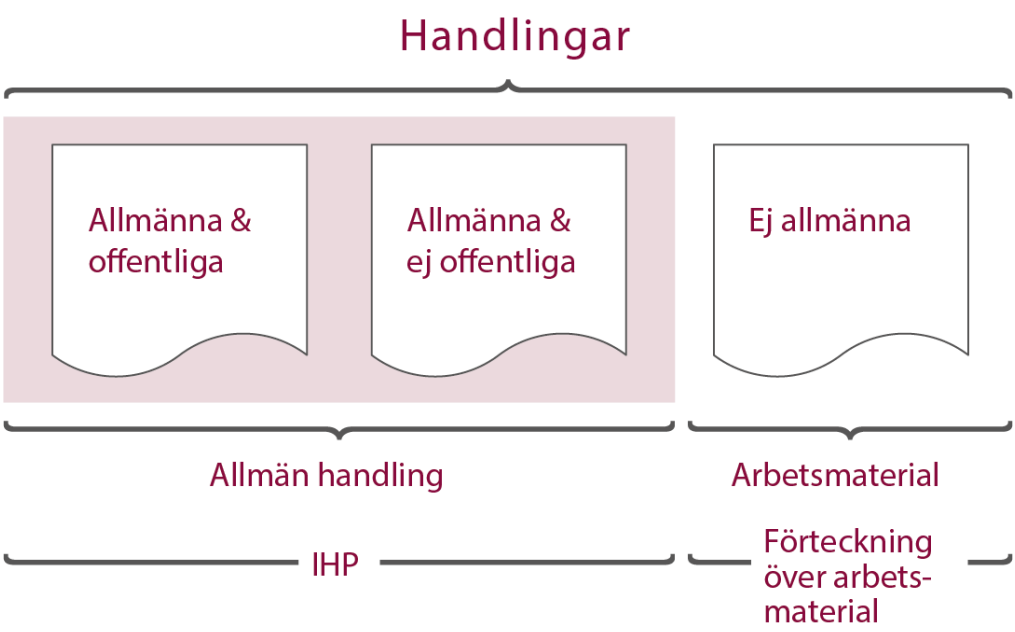
2.3.1 Allmänna handlingar och arbetsmaterial

En handling är allmän om den förvaras hos, är inkommen till eller upprättad av kommunen. Allmänna handlingar kan vara analoga eller digitala och de ska hanteras, bevaras och gallras enligt respektive verksamhets informationshanteringsplan (IHP).

En allmän handling är antingen offentlig eller sekretessbelagd. Alla allmänna handlingar som inte innehåller sekretessbelagd information är offentliga handlingar. Av olika anledningar kan handlingar vara helt eller delvis sekretessbelagda och det är upp till myndigheten (nämnden) att pröva frågan om sekretess.

Arbetsmaterial omfattas, till skillnad mot allmänna handlingar, inte av offentlighetsprincipen. Oavsett om informationen är en del av ett arbetsmaterial eller är en allmän handling, ska informationen informationsklassas. Kommunen har samma skyldighet att skydda information i ett arbetsmaterial som i en allmän handling. Arbetsmaterial finns i alla informationssäkerhetsklasser.

Handlingar



Figur 13. Handlingar (informationstyper) hos kommunen samt förhållandet till IHP. I figuren syns tre kategorier utav handlingar “Allmänna & offentliga”, “Allmänna och ej offentliga”, som tillhör gruppen allmän handling som i sin tur tillhör IHP, och “ej allmänna” som ligger under arbetsmaterial i förteckning över arbetsmaterial.

Varje verksamhet inom kommunen har en informationshanteringsplan (IHP). Arbetsmaterial definieras och dokumenteras i en kompletterande för-teckning över arbetsmaterial. I både IHP och i förteckningen över arbetsmaterial går det att utläsa hur de olika informationstyperna har informationsklassats.

Allmänheten ska kunna ta del av de allmänna handlingar som är offentliga. I vissa fall har en enskild person rätt att ta del av handlingar som innehåller sekretessbelagd information, vanligtvis om den egna personen (t.ex. en patientjournal).

Kommunen är skyldig att efter sekretessprövning ge allmänheten tillgång till en offentlig handling och skyndsamt tillhandahålla den i läsbar form till den som begär det. Sekretessprövning sker enligt offentlighets- och sekretesslagen; vid sekretessprövningen spelar därför informationens klassning ingen roll.

Utlämnande av allmän handling är lagstyrt

Observera att informationsklassen för konfidentialitet inte har någonbetydelse vid utlämnandet av en allmän handling. Dock ger klassen en indikation på att informationen kan innehålla sekretessbelagd uppgift eller känsliga personuppgifter, vilket påverkar om handlingarna kan lämnas ut och i så fall hur.

Information som klassats som **stark sekretess** men som vid en sekretessprövning inte bedöms innehålla sekretessuppgifter ska alltså lämnas ut skyndsamt om någon begär detta. Om en enskild person vill få en kopia av en allmän handling kan dock lagstiftningen direkt och informationsklassningen indirekt påverka på vilket sätt handlingen lämnas ut. Exempelvis kan handlingen lämnas ut via rekomenderad post med mottagningsbevis men inte via e-post (se även kapitel 2.13 – Hanteringsregler för olika konfidentialitetsklasser).

En sådan prövning görs enbart utifrån lagstiftningen, inte utifrån informationssäkerhetshandboken. Enbart klassningen av informationstypen visar inte om informationen är offentlig eller sekretessbelagd. Klassningen visar heller inte om informationen är ett arbetsmaterial eller en allmän handling. En medborgare har enbart rätt att ta del av allmänna handlingar eller uppgift ur allmänna handlingar, inte arbetsmaterial. Enligt offentlighets- och sekretesslagen ska ett utlämnande prövas varje gång en handling eller uppgift begärs ut.

Om begärd information har en hög informationsklass för konfidentialitet är detta en indikator på att informationen kan innehålla sekretessbelagd uppgift. Dataskyddsförordningen och i viss mån denna tillämpningsanvisning, kan påverka hur den begärda informationen lämnas ut. Om en enskild person vill få en kopia av en allmän handling kan dock lagstiftningen direkt och informationsklassningen indirekt påverka på vilket sätt handlingen lämnas ut. Exempelvis kan handlingen lämnas ut via rekommenderad post med mottagningsbevis men inte via e-post. Mer information om hantering av begäran om allmän handling finns i kommunens ärendehandbok.

2.3.2 Begreppen sekretess och konfidentialitet

Begreppen sekretess och konfidentialitet syftar till samma sak och båda begreppen relaterar till att information inte får avslöjas för obehörig. Användningen av begreppen skiljer sig dock åt. Begreppet sekretess tillämpas som juridisk term i lagtexter och reglerar vad som är en sekretessbelagd uppgift. En sådan uppgift får inte bli allmänt tillgänglig och tystnadsplikt råder för den som fått ta del av uppgiften.

Begreppet sekretess anger en viss nivå av juridiskt skydd. I klassningen har vi --ett behov av att kunna bedöma konsekvenser i flera nivåer. Vi har därför valt begreppet konfidentialitet för att beskriva hela bedömningen av hur infor-mationen ska hanteras inom kommunen.

Den som vill läsa mer om offentlighet och sekretess kan ta del av Linköpings kommuns ärendehandbok.

2.3.3 Informationsklassning och allmänna handlingar

Vid en informationsklassning görs en bedömning av de eventuella konsekvenser kommunen kan drabbas av om en viss informationstyp inte finns tillgänglig när den behövs, om den inte är rätt och riktig, om förändringar inte går att spåra eller om någon obehörig fått tillgång till informationen.

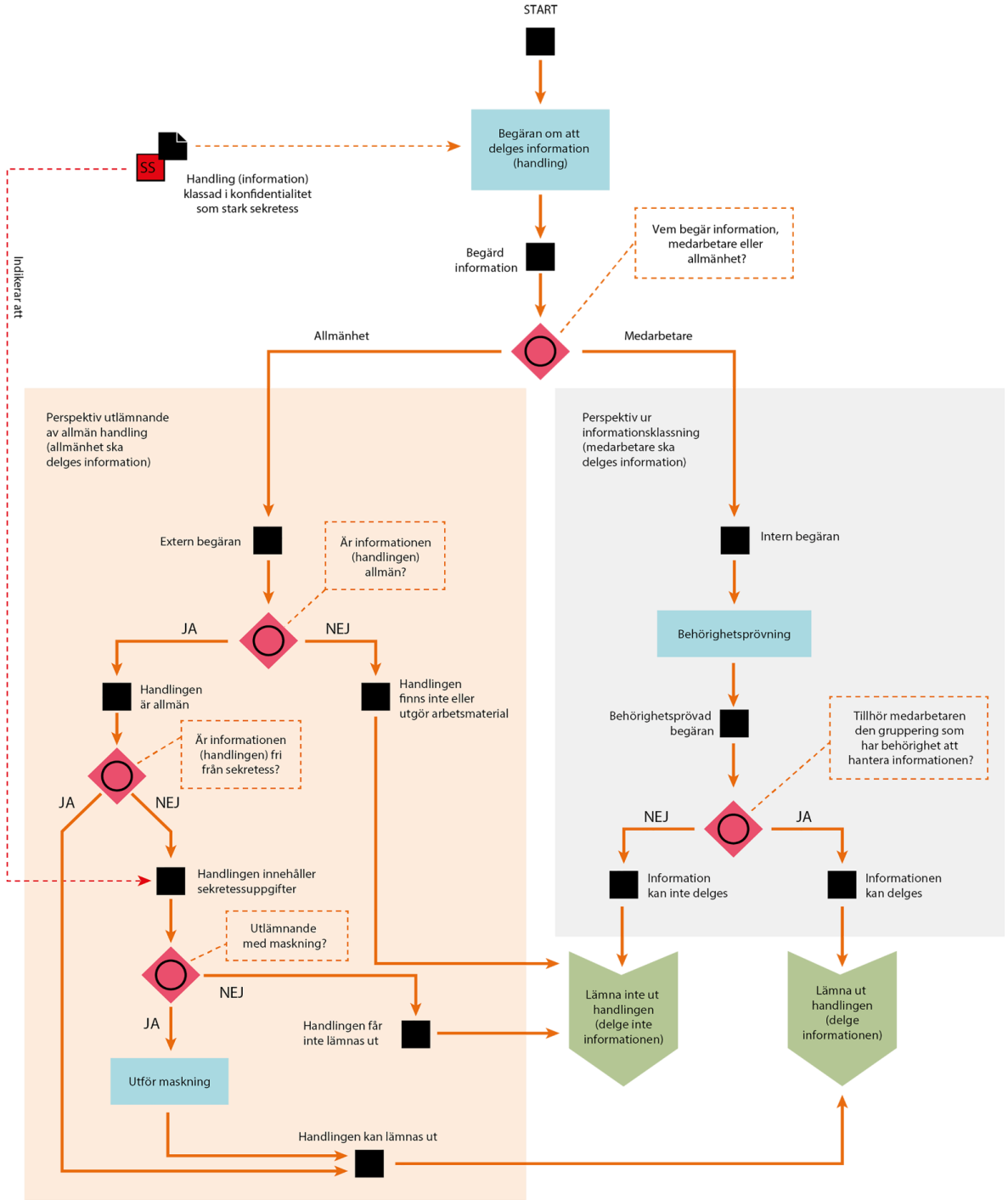
I informationsklassningen beaktas däremot inte om informationen är allmän handling eller om den är ett arbetsmaterial. Arbetsmaterial kan innehålla samma informationstyper som alla andra handlingar och kan därför leda till motsvarande konsekvenser vid klassningen.

Informationsklassningen omfattar alltså alla typer av handlingar i kommunen, inklusive arbetsmaterial.

Enbart klassningen av informationstypen visar inte om informationen är offentlig eller sekretessbelagd. Detta avgörs alltid i en sekretessprövning, oavsett vilken information som begärs ut. Enligt offentlighets- och sekretesslagen måste ett utlämnande prövas varje gång en handling eller uppgift begärs ut.

Bild: Bilden ovan föreställer en situation där en person visar information för en annan person. Det är en illustration till "utlämning av offentlig handling". Bilden visar två personer som arbetar vid ett bord. På bordet ligger det böcker och dokument. Mannen pekar på ett papper.

Figur 14 nedan visar skillnaden i handhavande mellan att en medarbetare i kommunen ska delges information (i exemplet klassad stark sekretess) och att en allmän handling med samma information ska lämnas ut till allmänheten.



Figur 14. Exempel på utlämnande av information (en handling) ur två perspektiv; informationens klassning (i exemplet stark sekretess) indikerar om handlingen innehåller sekretessuppgifter. Figuren illustreras en processkarta, som börjar med en handling, en begäran om att delges information.

Begäran delas sedan upp i två perspektiv (Allmänhet och Medarbetare), beroende på vem som begärt informationen.

Allmänhet: En extern begäran som antingen är allmän eller inte. Vid allmän handling lämnas informationen ut direkt. Är informationen allmän men inte fri från skretess, slussas den vidare till utlämning för maskning. Om informationen inte är en allmän handling och inte utgör arbetsmaterial, får denna inte lämnas ut.

Medarbetare: En intern begäran som genomgår en behörighetsprövning. Om medarbetaren tillhär grupperingen att ha behörighet kan informationen lämnas ut. Om medarnetaren inte har behörighet får informationen inte lämnas ut.

2.3.4 Informationsklassning och personuppgifter

I stort sett samtliga kommunens verksamheter hanterar personuppgifter, och dessa ska behandlas enligt dataskyddsförordningen och verksamhetsspecifika lagstiftningar.

Dataskyddsförordningen (GDPR) är en EU-förordning som syftar till att skydda registrerade personers personuppgifter. Integritetsskyddsmyndigheten är tillsyns-myndighet. Dataskyddsförordningen innebär bl.a. att kommunen ska

- kunna lämna information till en registrerad om vilken informationvi har om personen och den som personen är vårdnadshavare för
- i vissa fall kunna rätta felaktiga personuppgifter och komplettera med relevanta uppgifter som saknas
- i vissa fall kunna ta bort information när en registrerad person återkallar ett tidigare samtycke
- bara hantera och lagra personuppgifter där det finns rättslig grund för detta (t.ex. avtal och rättsliga förpliktelser) eller när kommunen fått samtycke
- anmäla personuppgiftsincidenter till Integritetsskyddsmyndigheten
- skydda personuppgifter med lämpliga säkerhetsåtgärder; reglerna i denna handbok är en del av skyddet.

Personuppgifter ska hanteras enligt den konsekvens det kan få för den enskilda personen, och uppgifter kan vara klassade som stark sekretess, sekretess, intern eller öppen information. Känsliga personuppgifter enligt dataskyddsförordningen klassas oftast som information med sekretess nivå 2 i konfidentialitet. Dit räknas uppgifter som röjer

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- sexualliv eller sexuell läggning
- genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Känsligheten i personuppgifter kan även bero på andra faktorer. Hänsyn måste därför tas till mängden uppgifter om en och samma person, eftersom den bestämmer hur detaljerad bilden av en person blir. Det innebär att flera personuppgifter som var för sig inte bedöms som känsliga tillsammans kan bilda känsliga personuppgifter. Notera även att personnummer endast får behandlas om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl.

Skyddade personuppgifter[3], dvs. personuppgifter med sekretessmarkering eller skyddad folkbokföringsuppgift, omfattas av sekretess och bör därför klassas som information med stark sekretess. Skyddade personuppgifter hanteras ofta med särskilda regler och anvisningar.

[3] Du kan läsa mer om skyddade personuppgifter hos Skatteverket (www.skatteverket.se).

Informationsklassning är inte bara konfidentialitet

När informationsägaren utför informationsklassningen bedöms samtliga fyra informationssäkerhetsperpektiv, alltså inte bara skyddsbehovet för konfidentialitet.
Även informationstypens skyddsbehov för riktighet, tillgänglighet och spårbarhet bedöms separat och tilldelas ett skyddsbehov.
Bedömningen för konfidentialitet återspeglar konsekvensen vid ett röjande av informationen. På samma sätt bedöms konsekvensen om informationen inte är riktig eller aktuell (riktighet), inte finns att tillgå (tillgänglighet) eller inte går att spåra eller återskapa (spårbarhet). En komplett informationsklassningen för en informationstyp består alltså av fyra värden som representerar informationens samlade skyddsbehov, exempelvis 0, 2, 3, 2 eller 4, 3, 3, 2.

De skyddsåtgärder som sedan införs för att tillfredsställa skyddsbehovet representerar faktiska skyddsnivåer utifrån alla fyra informationssäkerhetsperspektiv, exempelvis skyddsnivå 3 för konfidentialitet, skyddsnivå 2 för riktighet, skyddsnivå 1 för tillgänglighet och skyddsnivå 2 för spårbarhet. Observera att endast ett av perspektiven på skyddsnivå – konfidentialitet – är namnsatt (öppen, intern, sekretess och stark sekretess). De övriga tre perspektiven namnges endast med en siffra.
Om du vill läsa mer om hur kommunens modell för informationsklassningen fungerar, se kapitel 3.7 – Informationsklassning i Linköpings kommun. Kapitel 2 (detta kapitel) behandlar främst konfidentialitet eftersom detta perspektiv berör de flesta medarbetare. De andra tre perspektiven (riktighet, tillgänglighet och spårbarhet) bedöms och hanteras vanligen av specifika roller i kommunen och exponeras inte lika mycket för dig som medarbetare.

Exempel på informationstyper	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
Skolmat (Ingredienser)	0	3	1	2
Öppettider badhus	0	1	1	0
Personalakt	2	2	1	2
Familjeutredning	3	2	2	2
Leverantörsambud	2	3	1	2

Figur 15. Exempel på informationstyper och deras associerade kompletta informationsklassning.

2.4 Säkert beteende

En stor del av kommunens information hanteras både muntligt och skriftligt på papper och på skärm. Vi kommunicerar dagligen både informellt och formellt, och det är viktigt att agera med försiktighet och eftertanke när information med sekretess och stark sekretess hanteras.

Tänk på att det alltid finns information som inte är definierad eller klassad på förhand utan som skapas i samma ögonblick som informationen uttalas eller skrivs. Det är viktigt att varje medarbetare kan göra en preliminär bedömning av vilken informationsklass informationen tillhör, och kunna hantera den därefter. Man kan inte hantera information vårdslöst bara för att den inte hunnit få en formell informationsklassning ännu.

Om den nya informationen bedöms finnas kvar i verksamhet mer än tillfälligt så bör medarbetaren informera chef eller arkivredogörare om den nya informationstypen så att IHP kan uppdateras.
Försök att minimera omfattning av och antal uppgifter i ditt arbete, dvs. arbeta aktivt med uppgiftsminimering och undvik att spara information längre än nödvändigt.

Kretsen av behöriga personer är alltid begränsad för information med sekretess och stark sekretess. Därför är det viktigt att inga obehöriga kan uppfatta sådan information utanför och i arbetssituationer på arbetsplatsen eller i mer informella sammanhang, t.ex. vid samtal runt fikabordet eller när du pratar i telefon med en kollega på tåget.

Vid arbete i öppna kontorsmiljöer är det viktigt att tänka på att personer man har omkring sig kanske inte är behöriga att ta del av den information man hanterar. Det är därför viktigt att man uppsöker skyddade platser när information med höga skyddsbehov diskuteras muntligt eller i telefon. Vid arbete med bildskärm och papper i öppna miljöer ska hänsyn tas så att obehörig ej kan ta del av informationen.

ID	Regler och anvisningar för hantering av information muntligt, på papper och på skärm
M 4.1 	**Öppen** information är alltid tillåten att läsa och kommunicera utanför arbetsplatsen, t.ex. vid samtal på tåget eller telefonsamtal i kassakön.
M 4.2 	**Intern** information är tillåten att läsa och kommunicera om inte obehöriga är närvarande. Utanför kommunens lokaler ska läsning och kommunikation ske avskilt med försiktighet och eftertanke.
M 4.3 	Hantering av information med ***sekretess*** och **stark sekretess** ska -alltid ske avskilt från obehöriga samt med försiktighet och eftertanke. Vid -hantering av information med stark sekretess utanför kommunens -lokaler ska skydd mot insyn säkerställas.
M 4.4 	Information med sekretess samt stark sekretess får du endast kommunicera till den begränsade gruppens behöriga. Sådan kommunikation ska alltid utföras avskilt, så att med- eller avlyssning försvåras.
M 4.5 	Om du använder teknisk utrustning (telefon, dator eller liknande) för att kommunicera information med **sekretess** samt stark sekretess, får du endast använda en godkänd tjänst som kan begränsas till -gruppen behöriga.
M 4.6 	Skriftligt material som innehåller information med sekretess får du ha liggande- framme om inte andra än den begränsade gruppen kan ta del av materialet. I annat fall ska den döljas, t.ex i skåp eller skrivbordslåda.
M 4.7 	Skriftligt material som innehåller information med ***stark sekretess*** får inte ligga framme så att obehöriga kan läsa den. Lås in materialet i god-kända säkerhetsskåp när du lämnar arbetsplatsen, även kortare stunder.
M 4.8 	Information med ***sekretess*** och ***stark sekretess*** på datorskärm ska vara skyddad från obehöriga. Lås din skärm när du lämnar den, även kortare stunder. Om du har ett s.k. smartkort till datorn ska detta tas ut när du lämnar arbetsplatsen.
M 4.9 	Du ansvarar för dina besökare så länge de befinner sig i kommunens verksamhetslokaler. Besökare får inte vistas utan uppsikt i verksamhetslokaler där information med sekretess eller stark sekretess kan finnas tillgänglig. Obekanta personer i sådana lokaler ska alltid tillfrågas vem de söker och hjälpas tillrätta.

ID	Regler och anvisningar för hantering av information muntligt, på papper och på skärm
M 4.10 1 2 3	Vid extern posttjänst [4]ska du använda förslutna kuvert för information med **sekretess** och **stark sekretess**. Använd rekommenderade för-sändelser med mottagningsbevis om brev innehåller information med stark sekretess.
M 4.11 3	Vid intern posttjänst [5]ska du använda förslutna kuvert om brev innehåller information med **stark sekretess**. Placera kuvertet i -internpostmappar.
M 4.12 2 3	När information med sekretess eller stark sekretess skickas via fax ska du försäkra dig dels om att informationen skickas till rätt mottagare t.ex. genom att använda dig av kortnummer, dels om att mottagarens fax är övervakad med rätt mottagare vid överföringstillfället. Faxen får inte lämnas innan överföringen är klar. Överföring via fax ska ske undantagsvis; använd i stället funktioner med bättre säkerhet.
M 4.13 2	Vid utskrift av information med sekretess ska du övervaka utskriften om andra än den begränsade gruppen har tillgång till skrivaren. Alternativt används funktion för säker utskrift. Utskrift eller kopiering på offentliga skrivare eller kopiatorer [6]är inte tillåtet.
M 4.14 3	Vid utskrift av information med stark sekretess ska utskriften övervakas så att du är säker på att ingen obehörig kan läsa informationen. Alter-nativt används funktion för säker utskrift. Utskrift eller kopiering på offentliga skrivare eller kopiatorer är inte tillåtet.
M 4.15 2 3	Pappersdokument som innehåller information med sekretess och stark sekretess måste strimlas eller kastas i godkända säkerhetskärl.
M 4.16 0 1 2 3	Hårddiskar, cd/dvd, usb-minnen och andra liknande elektroniska -lagringsmedia ska lämnas till LKDATA för destruktion. Lagringsmedia som innehåller information med sekretess eller stark sekretess ska -rensas innan media lämnas till LKDATA.

2.4.1 Säkerhet och beteende vid din it-arbetsplats

Kommunen tillhandahåller godkända it-tjänster, bl.a. olika modeller av stationära eller bärbara it-arbetsplatser som möter kommunens krav och de behov som finns i verksamheten. It-arbetsplatserna kan antingen vara personliga eller delas mellan flera

[4] Extern posttjänst är post där en extern organisation (Postnord, lokalt postbud, DHL och liknande) ansvarar för postleveransen.
[5] Intern posttjänst är post som skickas med kommunens egna utförare för postleverans.
[6] Med offentlig skrivare eller kopiator menas utrustning som står i offentlig miljö och som kommunen inte ansvarar för.

medarbetare. En särskild typ av arbetsplats kan placeras i offentliga rum och får användas av allmänheten.
Alla it-arbetsplatser underhålls löpande för att ha hög säkerhet. Det är dock inte möjligt att skydda mot allting med enbart tekniska metoder. Användning av it-arbetsplatser ska därför ske med omdöme, ansvarskänsla och enligt gällande regler.
Kommunens datorer, programvaror och it-system är vanligen anpassade för att hantera olika typer av information med varierade klassning. Om du tar ut information ur ett it-system eller kopierar och överför den till ett annat it-system, andra media, annan lagring eller annat format finns en risk att du placerar informationen på ett ställe som inte kan upprätthålla den säkerhet som krävs. Undvik därför att avlägsna, flytta eller kopiera information ur den miljö där den är avsedd att behandlas. T.ex att kopiera ut information från ett verksamhetssystem och lägga den i en samarbetsplattform, eller att skriva ut och spara sådant som inte måste skrivas ut. Att avlägsna information från dess avsedda miljö kan också vara ett brott mot regler och anvisningar enligt denna handbok.

ID	Regler och anvisningar för användning av it-arbetsplats
M 4.17 0 1 2 3	Det är inte tillåtet att försöka få tillgång till information som du inte har rätt till.
M 4.18 0 1 2 3	Det är inte tillåtet att använda någon annans inloggningskonto.
M 4.19 0 1 2 3	Det är inte tillåtet att förstöra eller förvanska information som du är skyldig att spara eller störa system där informationen hanteras.
M 4.20 0 1 2 3	Det är inte tillåtet att uppenbart slösa med tillgängliga resurser, t.ex. arbetstid, maskinvara, programvara eller nätverk.
M 4.21 0 1 2 3	Du får inte ändra inställningar i utrustning vid it-arbetsplatser i syfte att kringgå regler och anvisningar i denna handbok.
M 4.22 0 1 2 3	Du får inte installera programvaror som bryter mot kommunens regler eller som inte är arbetsrelaterade på utrustning vid it-arbetsplatser. LKDATA övervakar alla installationer i kommunens utrustningar.
M 4.23 0 1 2 3	Du får inte bryta mot de licensregler som vanligen följer en programvara.

M 4.24 	Du får inte avlägsna digital information från den miljö där den är avsedd att lagras och behandlas, utom när den enligt regler ska gallras.

2.5 Identifiering, inloggningskonton och behörigheter

Det är viktigt att skilja på begreppen identitet och inloggningskonto. En identitet kan alltid kopplas till en fysisk person medan ett inloggningskonto är en behörighet, inte ett identitetsbegrepp. Du behöver bevisa din identitet för att få tillgång till ett inloggningskonto. Flera identiteter kan dessutom dela på ett inloggningskonto (gruppkonto), vilket då är en opersonlig behörighet till en resurs, t.ex. en funktionsbrevlåda eller en delad mobiltelefon.

Kombinationen inloggningskonto och lösenord är vanlig för att logga in i de flesta av kommunens it-system. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ett inloggningskonto och dess lösenord kan den personen komma åt användarens information och utföra aktiviteter i användarens namn. Att använda falsk identitet kan vara brottsligt.

I denna handbok regleras inloggningskonto och lösenord till kommunens nätverk medan inloggningskonton och lösenord för olika it-system och e-tjänster regleras av respektive systemförvaltning (inte att förväxla med förvaltning i kommunens organisation).

Lösenord ska bytas minst var 180:e dag. När det är dags får du en påminnelse när du loggar in och kan byta det själv. Observera dock att vissa it-system och e-tjänster saknar automatisk påminnelse för lösenordsbyte. Då ansvarar du själv för att bytet sker minst var 180:e dag. Kontrollera med din närmaste chef om du är osäker på huruvida de system och tjänster du använder har automatisk påminnelse eller inte.

Inloggningskonto och lösenord används för att skydda information som kan vara intern, sekretess eller stark sekretess.

Inloggningskonton och lösenord är viktig information. Ett inloggningskonto klassas som intern information där medarbetare inom kommunen kan delges benämningen (namnet) på ett inloggningskonto. Däremot är lösenord klassade som information med stark sekretess och får under inga omständigheter delas med andra.

ID	Regler och anvisningar för utformning av lösenord
M 5.1 	Dina lösenord ska vara minst 12 tecken långa. Ett lösenord till inloggningskonto med särskilda behörigheter ska vara minst 16 tecken långt.
M 5.2 	Du får inte skapa svaga lösenord, t.ex. genom att använda ● upprening av samma tecken: AAAAA ● logiska sekvenser: 123456, qwerty ● kända personliga fakta: namn, bilmärke ● ändring av enstaka tecken: hemligtlösen01, hemligtlösen02 osv.

Informationsruta

Tänk på följande när du skapar eller hanterar lösenord Ett lösenord ska vara svårt att gissa för någon annan och det ska inte kunna förknippas med dig som person. Lösenordet bör vara så långt (minst 12 tecken) och slumpmässigt som möjligt. Alla tecken på tangentbordet kan användas i ett lösenord. En bra metod är att sätta samman ord i meningar. Felstavningar, specialtecken och blandning av versaler och gemener och ord från olika språk ökar säkerheten ytterligare.

Här följer några exempel på bra och säkra lösenord som är lätta att komma ihåg och en variant som gör lösenordet ännu säkrare:

Bra och säkra lösenord

Vältalighet är en dygd

Jag gillar tulpaner!

3 eller 4 djupa andetag?

Peppar blå regn ost

Jag Ska Hem Nu!

Ännu säkrare variant

välTalighet ärEn dYgd

I like tulpaner!

treeller4djupaandetag?

pe77ar blå r3gn 0st

J4§ 5k4 H3m Nu!

För bästa säkerhet är det lämpligt att använda godkända lösenordshanterare för att skapa både säkra och olika lösenord till olika webbtjänster och till olika system inom kommunen.

Observera att lösenordet till hanteraren ska uppfylla reglerna M5.1 och M5.2. (Se Linweb för information om tillåtna lösenordshanterare.)

Lösenord fungerar olika i kommunens olika it-system. I vissa system kan lösenorden innehålla Å, Ä, Ö och alla specialtecken, medan andra system inte klarar det. Olika it-system kan dessutom vara sammankopplade så att det lösenord du använder först automatiskt skickas vidare till nästa system. Då måste lösenordet fungera i båda systemen. Använd bara tecknen a–z, A–Z och 0–9 om du vill vara säker på att ett lösenord fungerar i alla it-system.

ID	Regler och anvisningar för hantering av inloggningskonton och lösenord
M 5.3 0 1 2 3	Det är förbjudet att dela användningen av ditt personliga inloggningskonto. Använd alltid din personliga inloggning även om du delar dator med någon annan medarbetare.
M 5.4 0 1 2 3	Ditt lösenord ska aldrig förvaras åtkomligt för andra. Behandla lösenordet som en värdehandling som inte ska skrivas ner eller klistras upp på en lapp så någon kan komma åt informationen. Lösenord förvaras bäst i ditt minne eller i någon lösenordshanterare (se M5.8).
M 5.5 0 1 2 3	Du ska använda olika lösenord privat och i jobbet. Använd i första hand ditt Google-konto för registreringar på jobbrelaterade e-tjänster. När det inte är möjligt ska du använda unika lösenord för varje e-tjänst.
M 5.6 0 1 2 3	Byt lösenord omedelbart om du misstänker att det har röjts. Om du misstänker att någon annan använt ditt lösenord så ska du anmäla det som en säkerhetsincident.
M 5.7 0 1 2 3	Om du använder ett gruppkonto, nyttja inte automatisk minnesfunktion för lösenord till privata webbsidor.
M 5.8 0 1 2 3	Lösenordshanterare är tillåtet och kan användas. Denna ska ha ett lösenord som uppfyller M5.1 och M5.2 ovan. Se Linweb för information om tillåtna hanterare.
ID	Regler och anvisningar för hantering av inloggningskonton och lösenord
M 5.9	Byt lösenord manuellt minst var 180:e dag för it-system och e-tjänster som saknar automatisk påminnelse för byte av lösenord.

0 1 2 3	Du ansvarar själv för att detta byte sker.
M 5.10 0 1 2 3	För gruppkonton – dvs. konton där flera medarbetare använder samma inloggningskonto – gäller speciella regler och anvisningar där detta anges.

2.5.1 Nytt lösenord via Passwordkiosk

Du kan ändra lösenord via Passwordkiosk om du har glömt eller vill byta lösenord, förutsatt att du har registrerat ditt mobilnummer. Det finns flera sätt att nå Passwordkiosk, se Lindesk.

Om du inte har registrerat ditt mobilnummer kan du ta hjälp av två kollegor som intygar din identitet i Passwordkiosk och ger dig möjlighet att byta lösenord. LKDATA lämnar endast ut nya lösenord vid personligt besök och du måste kunna legitimera dig.

Detaljerade instruktioner för Passwordkiosk, t.ex. hur du registrerar ditt mobilnummer, finns i Lindesk.

2.6 Mobila enheter och arbete på distans

Kommunen tillhandahåller både stationära och mobila enheter. Som mobil enhet räknas bärbara datorer, surfplattor och smarttelefoner samt alla enheter som kan lagra digital information, t.ex. cd/dvd, usb-minnen, portabla hårddiskar och liknande.

Kommunen äger de smarttelefoner och surfplattor mm. som tillhandahålls medarbetaren för användning i tjänsten. Arbetsgivaren har rätt att ta del av information i enheter tillhörande kommunen– t.ex. e-post, sms, foton och -kalenderanteckningar – om det är nödvändigt för att kommunen ska uppfylla sin skyldighet enligt offentlighets- och sekretesslagen. Kommunen kan även ta del av de uppgifter som finns i den mobila enheten om det är nödvändigt vid fara för informationssäkerhetsbrott, t.ex. vid virus- eller hackerattacker eller för att utreda eller förhindra brott.

Mobila enheter används ofta vid arbete på distans, vilket kan påverka säkerheten. När du kopplar upp din mobila enhet i kommunens lokaler använder du kommunens gemensamma säkerhetslösningar, men dessa finns inte tillgängliga på samma sätt när du fjärransluter dig till arbetet via publika tjänster. Din mobila enhet är därför mer exponerad för säkerhetsrisker utanför kommunens lokaler. Var uppmärksam och följ de regler och anvisningar som anges på nästa sida.

Det är tillåtet att använda it-utrustning, t.ex dator eller mobiltelefon som du äger privat när du kör vissa av kommunens system som har godkänts för det. Gemensamt för godkända system är att ingen information lagras på din enhet. Informationen ligger hela tiden i kommunens system och du använder bara din egen enhet för att nå den. I vissa fall ställs olika krav på din dator eller telefon, t.ex att den är uppdaterad eller skyddas av lösenord. Vilka it-system som är -godkända att använda med egen utrustning kan du se på Linweb.

Alla instruktioner och regler om hur man arbetar med kommunens information gäller fortfarande när du använder egen utrustning. Det är t.ex inte tillåtet att ge någon annan tillgång till din inloggning eller att dela intern information med obehöriga. Det kan också finnas särskilda instruktioner för vissa system och då ska de följas. Om andra personer kan använda samma utrustning så måste du se till att den är utloggad från kommunens alla it-system varje gång du lämnar den.

Företag som arbetar på kommunens uppdrag kan också i många fall använda sin egen it-utrustning. Detta regleras i aktuella avtal.

Installation av appar (applikationer)

Var försiktig när du installerar appar eftersom de kan bryta mot kommunens regler. Vissa appar kan t.ex. dela din adressbok och kalender publikt eller sprida annan information utan din kontroll (se M2.1 och M6.7).

ID	Regler och anvisningar för hantering av mobila enheter
M 6.1	Mobila enheter som tillhandahålls av kommunen ska hanteras som personliga arbetsredskap. Du får inte låna ut eller överlåta dem om de inte är avsedda att delas av flera[7].
M 6.2	Mobila enheter ska alltid låsas upp med lösenord, pinkod, smartkort eller biometrisk inloggning, t.ex. fingeravtryck[8]. Smart kort eller bio-metrisk inloggning är rekommenderad metod. Ta för vana att låsa enheten om du inte använder den. Automatisk låsning sker efter tio minuters inaktivitet på de typer av enheter där detta är möjligt. En pinkod ska alltid bestå av minst sex siffror. Det är inte tillåtet med pinkoder som upprepar samma siffra (t.ex. 111111 eller 222222) eller som utgör logiska sekvenser (t.ex. 123456, 876543). Det är inte heller tillåtet att använda samma pinkod till olika plattformar, t.ex. till både telefon och passerkort.
ID	Regler och anvisningar för hantering av mobila enheter
M 6.3	Information med stark sekretess ska vara krypterad på mobila enheter. Om du hanterar information med stark sekretess i smarttelefon eller på surfplatta måste du använda en säkerhetslösning som godkänts av kommunen.

7 Gäller exempelvis beredskapstelefoner eller delade telefoner inom vård och omsorg.

8 Gäller enheter med funktioner för identifikation; alla enheter har inte denna funktion. Vissa enheter har installerade appar som hanterar verksamhetsinformation och som har funktion för identifikation.

M 6.4	Lagra aldrig information som på något sätt är arbetsrelaterad på endast en mobil enhet. Kopiera därför snarast över informationen till en lagringsplats som godkänts av kommunen.
M 6.5	Mobila enheter som inte ägs av kommunen kan anslutas till kommunens gästnät. Användaren måste då identifiera sig genom ett gästkonto. Missbruk leder till att gästkontot stängs av.
M 6.6	Vid distansarbete måste du använda kommunens godkända it-tjänster och anslutningar.
M 6.7	Du får inte installera applikationer (appar) vars innehåll eller funktion bryter mot kommunens regler.
M 6.8	Du kan använda privat utrustning för att ansluta dig på distans till kommunens godkända tjänster för arbete med öppen, intern och sekretess-information.

ID	Regler och anvisningar för fysisk hantering av mobila enheter
M 6.9	När privatägd eller delad utrustning används så måste man logga ut från alla kommunens e-tjänster när arbetet avslutas. T.ex. logga ut från Google Workspace i den privata datorn, innan någon annan använder den.
M 6.10	Iaktta försiktighet när du arbetar i publika miljöer. Skydda helst skärmen med insynsskydd.
M 6.11	Undvik arbete med information med sekretess i publika miljöer. Om det ändå är nödvändigt att göra det – arbeta avskilt så att informationen inte röjs för obehöriga.
M 6.12	Undvik arbete med information med stark sekretess i publika miljöer helt. Om det i undantagsfall är nödvändigt måste du vidta åtgärder (t.ex. insynsskydd på mobil enhet) och arbeta avskilt så att informationen inte röjs för obehöriga.
ID	Regler och anvisningar för fysisk hantering av mobila enheter
M 6.13	Lämna inte dina mobila enheter utan uppsikt. Förvara dem i säkert och skyddat utrymme.
M 6.14	Anmäl omedelbart förlust av mobil enhet till LKDATA och gör en polisanmälan – i vissa fall finns det möjlighet att fjärradera

	information.
M 6.15	Om anställning upphör eller (i vissa fall) om du byter arbetsuppgifter inom kommunen, ska mobila enheter återlämnas till LKDATA.
M 6.16	Vårda och hantera utrustningen på det sätt som föreskrivs i manual eller liknande, t.ex. genom att skydda den mot värme och fukt.
M 6.17	Om en privatägd utrustning som är inloggad i någon av kommunens e-tjänster förloras ska du omedelbart använda funktioner för att logga ut alla inloggade enheter och därefter byta lösenord.
M 6.18	Du får inte medföra it-utrustning eller lagringsmedia som innehåller kommunens information vid resor utanför EU/EES. Undantag kan beslutas av Säkerhetschef.
M 6.19	Du får inte logga in eller använda kommunens olika tjänster för -distansarbete vid resor utanför EU/EES. Undantag kan beslutas av Säkerhetschef.

2.7 Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram, t.ex. virus, trojaner, spionprogram eller maskar. Dessa kan installeras på en dator eller ett nätverk och har utvecklats i syfte att störa it-system, samla in information eller utnyttja datorkraft.

Skadlig kod är ett växande problem och kan vara svår att upptäcka. Angreppen blir dessutom allt mer sofistikerade och kan utföra allt mer avancerade operationer. I dag behöver man inte vara teknisk kunnig hacker för att skapa skadlig kod, utan det mesta som behövs kan köpas och beställas på olika marknadsplatser på internet.

Exempel på skadlig kod som förekommer i dag:

- trojaner som kan avlyssna -l-ösenord och skicka dessa vidare, s.k. keyloggers
- trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till information utan ägarens vetskap
- s.k. ransomware där filer eller diskar på datorer, smarttelefoner eller surfplattor krypteras och där en lösensumma krävs för att man ska komma åt filerna igen.

2.7.1 Spridning av skadlig kod

Skadlig kod kan spridas till datorer eller mobila enheter om du öppnar bilagor i e-post, importerar filer eller surfar på internet och klickar på infekterade länkar. Dessa infekterade länkar kan även finnas i sociala medier, t.ex. Facebook, Twitter eller Linkedin.

Avsändare till e-post kan enkelt förfalskas och webbsidor representerar inte alltid det som de utger sig för. Konton kan kapas, t.ex. på Facebook, och e-postadresser kan förfalskas i syfte att lura mottagaren att klicka på länkar.

Vid s.k. phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkontouppgifter. Var observant på dessa typer av händelser. Fyll aldrig i sådana uppgifter – seriösa myndigheter, företag och organisationer ber aldrig om uppgifter den vägen.

Det finns även en typ av e-post med förfalskad avsändare där mottagaren känner den som står som avsändare. Svarar man på ett sådant meddelande går svaret till angriparen som skickar nya svar tillbaka. Syftet är att mottagaren ska luras att göra saker som angriparen vill.

Ett av de bästa skydden mot skadlig kod är att vara medveten om potentiella hot och hela tiden bedöma rimligheten i det som händer på din skärm. Det gäller när du får e-post med länkar i, när du surfar och i alla andra sammanhang när du utbyter digital information med omvärlden. Kontakta alltid LKDATA för råd innan du klickar på något i ett e-postmeddelande som ser konstigt ut, kommer från en okänd avsändare eller innehåller bilder och länkar som är okända eller missvisande.

Skadlig kod, även via ett smittat usb-minne, kan sprida sig och orsaka stor skada om det kopplas upp mot kommunens nätverk. Kommunens datorer är utrustade med skydd mot skadlig kod, men utvecklingen på området är väldigt snabb så säkerheten är inte fullständig. Som medarbetare kan du bidra till ett bra skydd mot skadlig kod genom att följa nedanstående regler och anvisningar.

ID	Regler och anvisningar för skydd mot skadlig kod
M 7.1	Stäng aldrig av eller inaktivera installerat skydd mot skadlig kod.
M 7.2	Anslut endast godkänd it-utrustning till kommunens nätverk. Anslut inte portabla enheter som usb-minnen eller portabla diskar som misstänks vara smittade även om viss scanning efter virus alltid sker.
M 7.3	Var misstänksam. Klicka inte på okända eller konstiga länkar (där du inte kan säkerställa avsändaren) och fyll inte i uppgifter som verkar irrelevanta i sammanhanget.
M 7.4	Öppna endast bifogade filer om meddelandet kommer från en känd avsändare och du väntar på en bilaga. Misstänker du att avsändaren är förfalskad – kontakta din chef samt LKDATA.
M 7.5	Var observant på om it-utrustning beter sig långsamt eller konstigt. Kontakta LKDATA direkt om du misstänker att din it-utrustning smittats av skadlig kod.
M 7.6	Du får bara ansluta godkända USB-minnen eller andra portabla lagrings-enheter till kommunens it-utrustning. Kommunens USB--minnen och andra portabla lagringsenheter får inte anslutas till privatägd -utrustning som inte godkänts för det.

2.8 Digital kommunikation

Det finns många typer av digital kommunikation som via skrift, bild och ljud kan skickas inom kommunen och till externa mottagare. Exempel är Google Workspace, e-post och SMS. Regler och anvisningar för digital kommunikation gäller alla sådana funktioner.

Distansmöten, webbinarium m.m. är blandningar av visuell och muntlig kommunikation och de kan hållas både internt eller externt. Alla krav på informationssäkerhet gäller även i sådana sammanhang och för alla former av information, t.ex. ljud, text och bild. För att kontrollera vilka tjänster som är godkända att använda i respektive sammanhang, se Linweb.

Tänk på att allt som sägs, visas eller skrivs kan spelas in av varje deltagare, ibland även dolt för övriga deltagare.

2.8.1 Hantering av allmän handling vid digital kommunikation

E-post, chatt och motsvarande elektroniska meddelanden styrs av samma regler om offentlighet, sekretess, arkivering m.m. som traditionellt postbefordrade handlingar. Var och en som sänder eller tar emot information måste därför beakta vilken typ av information det handlar om och bedöma hur den ska hanteras.

Om du skickar eller tar emot en allmän handling via din e-postadress ska du bedöma om den ska diarieföras och i sådant fall lämna den till diariet, och ta bort handlingen ur e-posten. Om du behåller en kopia i din dator betraktas den därefter som arbetsmaterial.

E-post från enskilda personer eller från någon annan myndighet är i regel en allmän handling. Det kan även gälla e-post som skickas inom den egna organisationen. Är du osäker på om den allmänna handling som du fått eller upprättat ska diarieföras, läs i ärendehandboken eller kontakta registrator.

All e-post loggas centralt vad det gäller

- avsändare
- mottagare
- ärendemening
- tidpunkt och storlek på meddelandet
- namnet på bifogade filer.

Loggen sparas i 90 dagar enligt informationshanteringsplanen. Loggen är en allmän handling.

2.8.2 Att skicka intern information, information med sekretess och stark sekretess

Tänk på att digital kommunikation kan vara okrypterad. Om du skickar skyddsvärd information och behöver verifiera att informationen har anlänt korrekt kan du använda motringning via telefon för att bekräfta leveransen.

Du kan kontrollera e-postadressen för att skilja på vilka mottagare som är interna respektive externa. Alla e-postadresser som avslutas med ”@linkoping.se” eller “@utb.linkoping.se” har en intern mottagare. Avslutas e-postadressen på annat sätt är mottagaren extern. E-post som skickas internt [9]lämnar aldrig kommunens e-postsystem, vilket medför att vi själva kan kontrollera säkerheten i överföringen. Om e-post skickas utanför kommunen kan god säkerhet endast uppnås under vissa förhållanden, men vanligen sker överföringen öppet och utan insynsskydd.

Tänk på att aldrig skicka skyddsvärd information i e-postmeddelandets ärenderad eller kalenderinbjudningar eftersom denna information vanligen inte skyddas utan överförs öppet även om själva e-postmeddelandet i sig är krypterat.

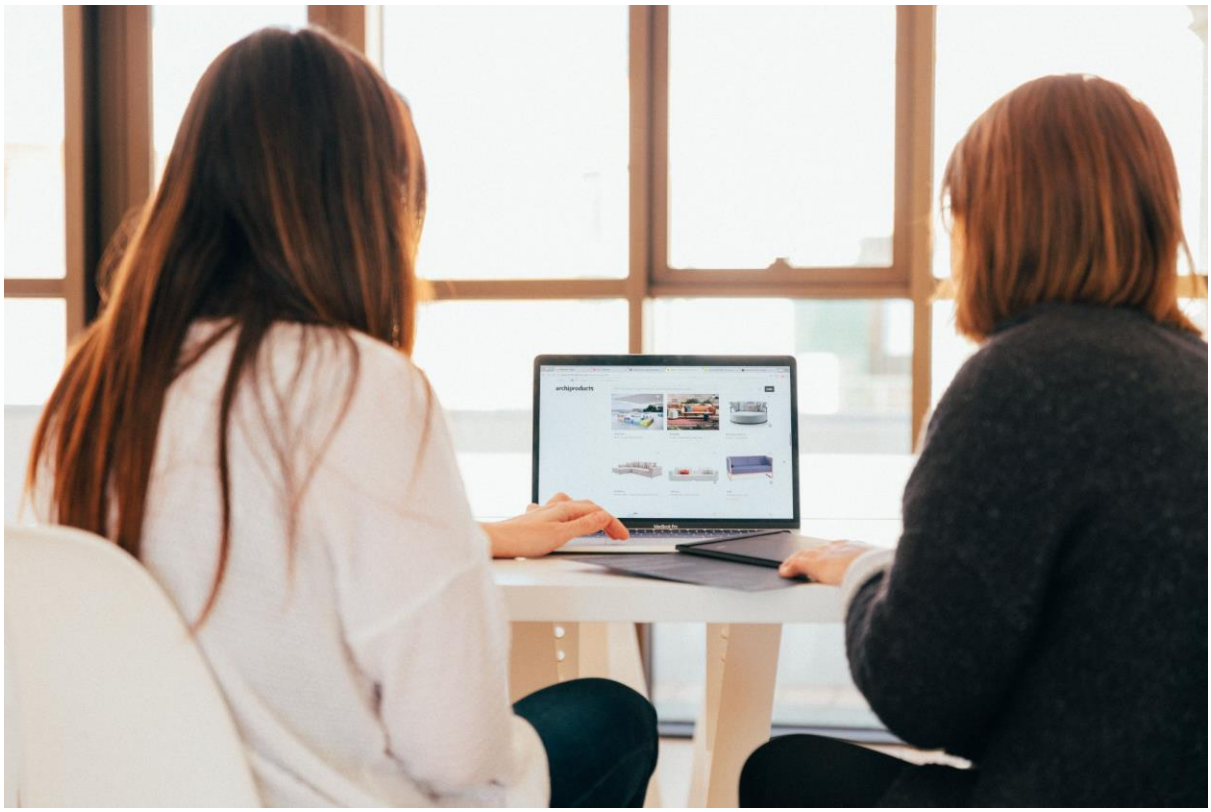
När du använder chatt, distansmöten m.m. kan det vara svårare att avgöra vilka mottagare som är externa och kontrollera vilka tjänster som är godkända att använda för respektive informationsklass. Om det råder minsta tveksamhet gäller försiktighetsprincipen. Tänk också på att det är ditt ansvar att verifiera att en mottagares e-postadress är känd, korrekt och gäller rätt person.

Undvik att vidarebefordra e-post utan att först noga kontrollera vad du skickar. Flera upprepade vidarebefordringar från medarbetare till medarbetare kan lätt skapa långa mejlkedjor där det kan vara mycket svårt att avgöra om delar av meddelandet innehåller

[9] Observera att e-postadresser som slutar med ”@edu.linkoping.se”; är externa.

skyddsvärd information. Motsvarande restriktioner bör användas när du skickar e-postkopior till andra mottagare, där du av misstag kan sprida information felaktigt.

Det finns olika tekniska lösningar för att möta verksamheternas behov av att skicka och ta emot information med stark sekretess, t.ex. kryptering av e-post. Dessa lösningar täcker dock inte in all e-post utan fungerar bara under vissa förutsättningar. Om du behöver skicka information med stark sekretess är det ditt eget ansvar att ta reda på hur det fungerar i respektive fall. Se Lindesk för mer information om hur du skickar information säkert.



Vad får delas med vem? Om du deltar i ett samarbete via en godkänd plattform, tänk på att vara noggrann med vilken informationen du delar (informationsklass). Var också uppmärksam på att det kan tillkomma deltagare i samarbetet som kanske inte har rätt att ta del av den information du delar.

2.8.3 Behörighet till e-post och kalender via ombud

I kommunens e-postsystem kan du låta en kollega hantera din e-post och din kalender via en funktion där du ger behörighet till ett eller flera namngivna ombud, t.ex. registrator. Detta ombud hanterar då din e-post och kalender i ditt namn eller enligt den behörighet som angetts. Beroende på typ av tjänst eller roll kan denna funktion vara lämplig att använda om du t.ex. är på semester och din e-post måste bevakas eller kalenderbokningar måste hanteras. Vi är skyldiga att kontrollera vår e-post varje arbetsdag.

Tänk på att den medarbetare som får behörighet normalt kan läsa och ta del av e-post och kalender utan begränsningar. Om du utbyter information i de högre klasserna av konfidentialitet är det därför lämpligt att meddela berörda avsändare att det inte är du som öppnar e-posten. Läs mer i Lindesk om hur du praktiskt ställer in funktionen för ombud till e-post och kalender.

ID	Regler och anvisningar för skydd mot skadlig kod
M 8.1 0 1 2 3	Du som är kontoinnehavare för ett individuellt e-postkonto är ansvarig för den e-post som skickas från kontot. Du är alltid skyldig att följa de ytterligare regler som framgår av kommunens e-postrutin.
M 8.2 0 1 2 3	Du ansvarar själv för att löpande öppna och läsa inkommande e-post till ditt e-postkonto. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska du lämna behörighet till en annan (eller flera andra) medarbetare. Meddela den som du delar information med sekretess och stark sekretess att det inte är säkert att det är du som hanterar e-posten.
M 8.3 0 1 2 3	E-postkonton som delas av flera, t.ex. funktionsbrevlådor, ska ha en utpekad person eller roll som ansvarig.
M 8.4 0 1 2 3	Alla nämnder och kommunstyrelsen ska ha en funktionsbrevlåda kopplad till och bevakad av diariet. Dessa funktionsbrevlådor ska bevakas varje arbetsdag. E-post som kommer till en sådan funktionsbrevlåda ska kvitteras.
M 8.5 0 1 2 3	Massutskick av e-post inom kommunen får endast göras om både närmaste chef och kommunikationsavdelningen godkänt detta. Externa massutskick får endast ske om dessa är tydligt relaterade till kommunens verksamhet (utskick om tomtkö, barnomsorg etc.).
M 8.6 0 1 2 3	Det är endast tillåtet att ange information som klassas som öppen i ett e-postmeddelandes ämnesrad eller i kalenderinbjudningar. Skriv aldrig t.ex. personuppgifter i detta fält.

ID	Regler och anvisningar för e-post

M 8.7 0 1 2 3	Var restriktiv med användningen av ”skicka kopia till”-funktionen (både öppen-/klartext kopia och hemlig kopia) så att du inte skickar information som inte är relevant för mottagaren. Vidarebefordra inte heller e-post med information som inte ska delas med andra, t.ex. personuppgifter eller sekretessbelagda uppgifter, med tanke på risken för mejlkedjor.
M 8.8 0 1 2 3	Var restriktiv med att vidarebefordra e-post utan att först noga kontrollera vad du skickar. Flera upprepade vidarebefordringar från medarbetare till medarbetare kan lätt skapa mejlkedjor där det är mycket svårt att avgöra om hela eller delar av meddelandet innehåller information med sekretess eller stark sekretess.

ID	Regler och anvisningar för allmänna handlingar i e-post
M 8.9 0 1 2 3	Du måste alltid bedöma om inkommande respektive utgående e-post är en allmän handling och hantera den enligt kommunens regelverk (se kommunens ärendehandbok).
M 8.10 0 1 2 3	E-post som är allmän handling får gallras, dvs. raderas, först när e-posten diarieförts, hålls ordnad på annat sätt eller om det finns ett gallringsbeslut. Gallring av allmänna handlingar regleras i respektive verksamhets informationshanteringsplan samt i särskilda gallringsbeslut från Stadsarkivet. För arbetsmaterial gäller att det normalt ska rensas när ärendet avslutats.

ID	Regler och anvisningar för privat e-post
M 8.11 0	Du får använda din kommunala e-postadress (@linkoping.se eller @utb.linkoping.se) privat, så länge det inte inkräktar på arbetet, medför kostnader eller på annat sätt skadar kommunen. Notera dock att all användning loggas och att loggarna normalt är att betrakta som allmän handling som kan begäras ut.
M 8.12 0 1 2 3	Du får inte använda privata e-postadresser för tjänsteärenden.
M 8.13 0 1 2 3	Du får inte använda ditt inloggningsnamn eller din kommunala e-postadress för registrering i någon e-tjänst som du använder privat.
M 8.14 2 3	Du får inte automatiskt vidarebefordra e-post från din kommunala e-postadress (@linkoping.se eller @utb.linkoping.se) till externa e-postadresser.

Informationsklass	Parter	E-post Kommunens godkända tjänster	Distansmöte (Kommunens godkända tjänster)	Chatt (Kommunens godkända tjänster)

Informations - klass 0-1 0 1	interna och externa parter	OK	OK	OK
Informations - klass 2 2	interna och externa parter	OK	OK	Nej
Informations - klass 3 3	interna parter godkända identifierade externa parter	OK	OK	Nej
	övriga externa parter	OK med filkrypto	Nej	Nej
	alla interna och externa parter - PDL - SoL-PuL - 18 kap 8 § OSL - 18 kap 9 § OSL - 18 kap 13 § OSL	OK med filkrypto	Nej	Nej

Tabell 4. Översikt av godkänd informationshantering i e-post, distansmöte och chatt avseende konfidentialitet.

ID	Regler och anvisningar gällande e-post, chatt, distansmöten eller andra meddelandefunktioner
M 8.15 3	För information som berörs av nedanstående gäller särskilda regler • PDL • SoL-PuL • 18 kap 8 § OSL • 18 kap 9 § OSL • 18 kap 13 § OSL Om det är nödvändigt i arbetet får du skicka sådan information, oavsett mottagare, i e-post om den placeras i ett bifogat dokument som har krypterats med kommunens godkända metod för kryptering av dokument, samt att du har överfört lösenordet till mottagaren på ett säkert sätt. Du får inte hantera sådan information oavsett mottagare i chatt eller i distansmöte.

ID	Regler och anvisningar gällande e-post, chatt, distansmöten eller andra meddelandefunktioner
M 8.16	Du får skicka information med stark sekretess till interna e-post-adresser i kommunen, dvs. till adresser som innehåller ”@linkoping.se” och

0 1 2 3	“@utb.linkoping.se” samt till vissa av kommunen godkända -organisationer under de förutsättningar som framgår av e-postrutinen. Statliga myndigheter, regioner och kommuner är alltid att betrakta som godkända organisationer. Övriga mottagare ska beredas av Informationssäkerhetsrådet och godkännas av Säkerhetschef. Det ska finnas en lista över godkända mottagare, se Lindesk. Om information med stark sekretess skickas till dig utan att ovanstående instruktioner följts ska du omgående meddela avsändaren om gällande regler och hänvisa till en korrekt hantering. Vid upprepade avsteg från gällande regler ska detta rapporteras som en incident. Om du behöver skicka information med stark sekretess till mottagare i organisationer som inte har godkänts enligt ovan så kan du skicka den med e-post i ett bifogat dokument som har krypterats med kommunens godkända metod för kryptering av dokument, samt att du har överfört lösenordet till mottagaren på ett säkert sätt.
M 8.17 0 1 2 3	Du får skicka information som är informationsklassad som öppen, intern eller sekretess till samtliga e-postadresser (externa och interna). När du ska skicka uppgifter med sekretess bör du överväga att skicka informationen i ett bifogat dokument som har krypterats med kommunens godkända metod för kryptering av dokument, samt att du har överfört lösenordet till mottagaren på ett säkert sätt.
M 8.18 0 1	Godkända tjänster för chatt får användas för att hantera information som har informationsklassats som öppen och intern med alla mottagare (interna och externa). Information som har informationsklassats med sekretess eller stark sekretess får inte hanteras i chatt oavsett mottagare (interna och -externa). Meddelandefunktioner i verksamhetssystem kan användas på den klassningsnivå som själva systemet är godkänt för.
M 8.19 0 1 2	Kommunens godkända tjänster för distansmöten får användas för att hantera information som har informationsklassats som öppen, intern eller sekretess oavsett deltagare i mötet under de förutsättningar som framgår av separat rutin för distansmöten.
M 8.20 3	Kommunens godkända tjänster för distansmöten får användas för att hantera information som har informationsklassats som stark sekretess när alla deltagare är interna (använder konton som slutar på @linkoping.se eller @utb.linkoping.se) samt till vissa av kommunen godkända organisationer under de förutsättningar som framgår av separat rutin för distansmöten. Undantaget information som berörs av regel M8.15

2.9 Internet och sociala medier

Förutom de regler och anvisningar som är kopplade till skadlig kod finns det särskilda regler och anvisningar för hur du ska använda internet och sociala medier i din yrkesroll.

Uttalanden på internet och i sociala medier kan påverka allmänhetens uppfattning både om dig som enskild person och om Linköpings kommun. När du uttalar dig som representant för kommunen är det därför viktigt att du gör det enligt kommunens regler och utifrån god etik och gott omdöme. Det måste vara tydligt om du uppträder som privatperson eller som företrädare för Linköpings kommun. För att använda sociala medier som en del av tjänsten ska det finnas ett tydligt beslut från verksamhetschef. Kommunens kommunikationspolicy och riktlinjer för kommunikation samt anvisningar för sociala medier ska följas vid sådan kommunikation.

Alla aktiviteter på internet till och från kommunens nätverk övervakas och loggas. Kommunen kan också blockera vissa typer av datatrafik som kan kopplas till nedanstående regler och anvisningar.

ID	Regler och anvisningar för internetanvändning
M 9.1 0 1 2 3	Internet är i första hand ett arbetsverktyg men du kan även använda det för privat bruk i sådan omfattning att ordinarie arbetsuppgifter inte störs. Din användning får inte innebära merkostnader för kommunen.
M 9.2 0 1 2 3	De lagar som gäller i samhället i övrigt gäller självklart även vid användning av internet. Exempel på lagar som berörs är tryckfrihetsförordningen, offentlighets- och sekretesslagen, dataskyddsförordningen, brottsbalken samt lagen om upphovsrätt.
M 9.3 0 1 2 3	Det är förbjudet att ladda ner och sprida upphovsrättsskyddade dokument, filer eller program utan rättighetsinnehavarens tillstånd.
M 9.4 0 1 2 3	Utrymmeskrävande filtyper för privat bruk, t.ex. filmer, program eller spel, får inte laddas ner, strömmas, lagras eller spridas i eller via kommunens nätverk.
M 9.5 0	Endast öppen information får publiceras eller överföras via internet, eftersom internet är ett öppet nätverk. Om information har högre informationsklass än öppen krävs särskilda skydd (se nästa regel).
M 9.6 1 2 3	För publicering eller överföring av information med intern, sekretess eller stark sekretess via internet krävs godkända tjänster (se Linweb om vilka tjänster som är godkända för att publicera eller överföra information i olika klasser).

ID	Etiska regler och anvisningar för internetanvändning
M 9.7 0 1 2 3	Du får inte besöka webbplatser med innehåll som uppmuntrar till t.ex. brottslig verksamhet, rasism, diskriminering eller våld eller som har ett pornografiskt innehåll.
M 9.8 0 1 2 3	Om du har ett uppdrag i din tjänst som kräver tillgång till information av den typ som omnämns i regel M9.7 krävs en formell ansökan om dispens signerad av närmaste chef. Ansökan ställs till kommunens informationssäkerhetsråd som behandlar ärendet. Denna typ av dispenser är alltid tidsbegränsade.
M 9.9 0 1 2 3	När du uppträder som representant för kommunen får du inte publicera något på internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt och finns kvar under lång tid. Tänk igenom innehållet noga innan du publicerar det.

Kommunen är aktiv på sociala medier och varje förvaltning har en kommunikationsorganisation[10]. De medarbetare som skriver i kommunens namn har kunskap om kommunikation och för dem gäller särskilda regler. Det är verksamhetens chef som ansvarar för att verksamhetens konton på sociala medier följer våra riktlinjer, anvisningar och övriga rutiner. När det gäller kommunövergripande konton på sociala medier är det bara kommunikationsstaben som kan och får publicera innehåll på t.ex. Facebook, Instagram, Twitter och Youtube.

Följ nedanstående regler och anvisningar när du är aktiv på sociala medier.

ID	Etiska regler och anvisningar för internetanvändning
M 9.10 0	För att använda sociala medier i sin tjänsteutövning krävs godkännande av verksamhetschef.
M 9.11 0	Om du har godkännande enligt M9.10 företräder du alltid kommunen. I övrigt bör det tydligt framgå när du företräder kommunen och när du ger uttryck för din egen åsikt.

[10] Se vidare i Kommunens kommunikationspolicy och Riktlinjer för kommunikation.

Bilden visar en Ipad och en telefon som ligger på tangentbordet på en bärbar dator.

2.10 Lagring och säkerhetskopiering

Det är viktigt att information lagras säkert och säkerhetskopieras regelbundet så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering eller liknande. LKDATA ansvarar för och tillhandahåller tjänster dels för att information säkerhetskopieras, dels för att informationen är möjlig att återställa.

Uppgifter som hanteras i verksamhetssystem ska främst hanteras i avsedda system, såsom Heroma, Treserva, W3D3 etc.

Information i konfidentialitetsklass stark sekretess kan tillfälligt hanteras på din egen eller delade enheter i Google Drive eller din egen dator. Övrig information kan hanteras på Google Drive eller i din egen dator så länge som den behövs för den löpande verksamheten, därefter ska den tas bort. Se separat hanteringsinstruktion på Linweb.

Lokal lagring i mobila enheter (samtliga typer) är endast tillåten om informationen också finns lagrad på någon annan godkänd plats. Tänk därför på att föra över informationen till en säker lagring snarast om du hanterar information i en mobil enhet.

Varje verksamhet ansvarar för att gallra information enligt gallringsbeslut eller verksamhetens informationshanteringsplan samt för att rensa arbetsmaterial.

Allting du raderar i Google Drive kan du själv återställa inom 30 dagar, därefter raderas den helt och kan inte återställas.

Om du gör ändringar i olika dokument som du sen vill återställa så finns funktioner för det i alla olika Google-verktyg. Funktionen kan variera beroende vilket verktyg det gäller.

ID	Regler och anvisningar för lagring och säkerhetskopiering
M 10.1 2 3	Lagra alltid information som används i verksamheten (allmänna handlingar och arbetsmaterial) på godkända lagringsplatser så att informationen säkerhetskopieras. Lagring av information ska i första hand ske i anvisade verksamhets-system. Under begränsad tid kan information också sparas i personliga eller delade enheter i Google Drive eller i mappen “Mina Dokument “ i kommunens datorer.
M 10.2 0 1	Lagring av information ska i första hand ske i anvisade verksamhets-system. Information kan också lagras i personliga eller delade enheter i Google Drive eller i mappen “Mina Dokument “ i kommunens datorer.Personuppgifter ska tas bort när de inte längre behövs.
M 10.3 2 3	Lokal lagring av information med sekretess och stark sekretess, t.ex. på en dator eller ett usb-minne, är endast tillåten om lagringsenheten eller filerna är krypterade med godkänd kryptering.
M 10.4 2	Fysiska pappersdokument som innehåller information med sekretess ska endast förvaras åtkomliga för en begränsad grupp.
M 10.5 3	Fysiska pappersdokument som innehåller information med sekretess ska förvaras inlåsta i säkerhetsklassade skåp (se Säkerhets--handboken samt kapitel 6 – Informationssäkerhet och fysiskt skydd för mer information).
M 10.6 0 1 2 3	Du kan använda USB-minnen för att flytta information men inte för permanent lagring. USB-minnet ska vara godkänt för den informationsklass som informationen har.

2.11 Molntjänster

Datormoln – även kallat molntjänster, molnet eller cloudtjänster – är it-tjänster som tillhandahålls över internet. Detta gäller ofta funktioner som traditionellt sköts på den egna datorn men genom molnet sköts av någon annan. Det kan till exempel handla om tillämpningsprogram, serverprogram och lagring av data.

Säkerhetskraven på molntjänster är desamma som på de it-tjänster som kommunen själv tillhandahåller. Detta medför att samtliga kommunens säkerhetskrav som kan tillämpas även gäller molntjänstleverantörer, t.ex. krav på konfidentialitet eller krav på att information alltid ska vara tillgänglig för kommunen utan att vara beroende av enskilda personer. Därför

måste alltid användning av molntjänster regleras i avtal mellan molntjänstleverantören och kommunen. Sådana avtal inklusive eventuella personuppgiftsbiträdesavtal får endast tecknas av behöriga företrädare för Linköpings kommun.

ID	Regler och anvisningar för lagring i molntjänster
M 11.1 0 1 2 3	Du får endast använda molntjänster som är godkända av kommunen och reglerade i avtal (se Linweb) vid behandling av kommunens information.
M 11.2 0 1 2 3	Du får endast använda molntjänster för den information och den informationsklass respektive tjänst är godkänd för. För varje godkänd molntjänst ska det finnas en förteckning över vilka informationstyper och vilken informationsklassning den är godkänd för (se Linweb).

2.12 Spårbarhet och loggning

Aktiviteter i kommunens datorer, nätverk och it-system loggas. Loggarna används för att felsöka och utreda incidenter och störningar samt för att förebygga brott. I vissa fall är kommunen enligt lag skyldig att logga och kontrollera loggarna. Loggarna lagras under en viss tid och är då endast åtkomliga för begränsade grupper av administratörer. Under vissa omständigheter kan loggar begäras ut och göras tillgängliga för andra, t.ex. chefer.

Spårbarhet innebär att man genom loggarna kan identifiera vem som har gjort vad och när samt följa förloppet för olika händelser. Vissa it-system har egna loggar och i vissa fall regleras dessa av särskild lagstiftning. Gallring av loggar sker enligt informationshanteringsplanen och gallringsbeslut.

Användning av internet registreras i en logg. Loggningen innefattar bl.a. uppgifter om användarnamn samt namn på den webbplats som besökts. Det förs även logg över all e-post med uppgifter om avsändare, mottagare, ärendemening, tidpunkt samt namn på bifogade filer.

Med hjälp av loggen kan kommunen kontrollera hur medarbetare använt internet. Vid denna kontroll sker ingen kontroll av enskilda individers användning.

De åtkomliga webbplatserna är indelade i olika kategorier, t.ex. sport, nyheter, spel eller pornografi. Om kontroller visar att det förekommer användning som bryter mot gällande regler, eller om användandet sker i onormalt stor omfattning, kan en förvaltningschef dock besluta om kontroll av enskilda individers användande.

Kommunen kan även ta del av uppgifterna i e-postmeddelanden om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet, om det är nödvändigt vid att hantera en fara för informationssäkerheten, t.ex. vid virus- och hackerangrepp, eller för att utreda eller förhindra brott.

Om kontrollerna visar att reglerna i denna handbok överträtts kan ärendet -komma att utredas.

De uppgifter som ligger till grund för kontrollen av anställdas internet- och e-postanvändning gallras efter tre månader. Om en utredning påbörjas sparas uppgifterna så länge utredningen pågår eller längre om händelsen leder till anmälan eller arbetsrättslig åtgärd.

Användningen av it övervakas av kommunen för att dels bibehålla it-systemens stabilitet, dels identifiera och förebygga incidenter. I denna övervakning kan kommunen dekryptera trafik i syfte att upprätthålla användbara loggar.

ID	Regler och anvisningar för spårbarhet och loggning
M 12.1 	Det är inte tillåtet är radera, förvanska eller på något annat sätt påverka loggar i kommunens it-system.

2.13 Hanteringsregler för olika konfidentialitetsklasser

Tabell 4 på nästa sida beskriver översiktligt vilka regler och anvisningar som gäller de vanligaste typerna av aktiviteter i kommunen. Syftet är att i stora drag redovisa vanliga situationer som du som medarbetare kan tänkas möta. Alla kommunens aktiviteter redovisas dock inte, så du kan behöva söka information i andra kapitel i handboken om hur du ska agera vid hantering av en viss informationstyp. Kontakta din närmaste chef för stöd om du behöver ytterligare vägledning.

Reglerna nedan är utformade med informationssäkerhet som utgångspunkt. Om regler för en viss typ av hantering saknas ska du agera ansvarsfullt och följa andra regler och anvisningar som gäller i din verksamhet.

I kolumnen längst till vänster återfinns referenser till vilken eller vilka regler och anvisningar som tillämpats i det specifika fallet.

Hanteringsregler – exempel på aktiviteter (situationer)	Informationsklass gällande konfidentialitet			
	0. Grön: Öppen information	1.Gul: Intern information	3.Orange: information med sekretess	4.Röd: information med stark sekretess
Fysiskt möte (muntliga samtal) (Ref.: M 4.1, M 4.2, M 4.4, F 5.4-6)	Inga restriktioner.	Ska ske med försiktighet och eftertanke.	Ska ske avskilt från obehöriga och med försiktighet och eftertanke.	Ska ske avskilt från obehöriga och med försiktighet och eftertanke. Säkerställ att ingen form av överhörning sker.
Telefonsamtal (Ref.: M 4.1, M 4.2, M 4.4, M 4.5)	Inga restriktioner.	Ska ske med försiktighet och eftertanke.	Ska ske avskilt från obehöriga samt med försiktighet och eftertanke.	Ska ske avskilt från obehöriga samt med försiktighet och eftertanke. Säkerställ att ingen form av överhörning sker.
Utskrift på skrivare eller kopiering i kommunens lokaler eller vid hemarbete (Ref.: M 4.13, M 4.14)	Inga restriktioner.	Ska ske med försiktighet och eftertanke. Utskrift bör övervakas.	Utskrift ska övervakas av behörig[11]. Alternativt används godkänd funktion för säker utskrift[12].	Utskrift ska ske på personlig skrivare och övervakas. Alternativt används godkänd funktion för säker utskrift.
Utskrift eller kopiering på offentliga[13] skrivare eller kopiatorer (Ref.: M 4.13, M 4.14)	Inga restriktioner.	Utskrift ska övervakas.	Är inte tillåtet.	Är inte tillåtet.

[11] Med behörig menas en person som ingår i en aktuell begränsad gruppering.
[12] Med funktionen säker utskrift lagras utskriften till dess att användaren kvitterar ut utskriften med ett personligt lösenord, en personlig kod eller annan typ av personlig identifiering.
[13] Med offentlig skrivare eller kopiator menas utrustning som står i offentlig miljö och som kommunen inte ansvarar för.

Hanteringsregler – exempel på aktiviteter (situationer)	Informationsklass gällande konfidentialitet			
	0. Grön: Öppen information	1.Gul: Intern information	3.Orange: information med sekretess	4.Röd: information med stark sekretess
Hantering av information på papper eller på skärm [14]i kommunens lokaler eller vid hemarbete (Ref.: M 4.1, M 4.2, M 4.3, F 5.4-6)	Inga restriktioner.	Inga restriktioner.	Ska ske avskilt samt med försiktighet och eftertanke.	Ska ske avskilt samt med försiktighet och eftertanke.
Hantering av information på papper eller på skärm i publik miljö (Ref.: M 4.1, M 4.2, M 4.3, M6.10, M6.11, M6.12)	Inga restriktioner.	Ska ske med försiktighet och eftertanke.	Ska ske avskilt samt med försiktighet och eftertanke.	Ska ske avskilt från obehöriga samt med försiktighet och eftertanke. Säkerställ att ingen form av överhörning sker.
Förvaring av pappersdokument. Gäller både på -arbetsplatsen och vid hemarbete (Ref.: M 4.6, M 4.7, M 10.4, M 10.5)	Inga restriktioner.	Tillträdesskydda t från obehörig.	Tillträdesskyddat från obehörig, förvaras i låst utrymme eller låst förvaring..	Utskrift ska ske på personlig skrivare och övervakas. Alternativt används godkänd funktion för säker utskrift.
Lagring av digital information (Ref.: M 6.3, M 10.1, M 10.2, M 10.3)	Ska ske i -godkänd tjänst.nga restriktioner.	Ska ske i godkänd tjänst.	Ska ske i godkänd tjänst/godkänt system där den begräns-ade gruppen har åtkomst.	Är inte tillåtet.
Vid resa: förvaring av informationsbärare i form av pappersdokument, dator, usb-minne, cd, dvd m.m. (Ref.: M6.10, M6.18, M6.19)	Inga restriktioner. Vid resa utanför EU/EES krävs godkännande av säkerhetschefe n.	Under personlig uppsikt eller inlåst i rum, skåp eller liknande. Vid resa utanför EU/EES krävs godkännande av säkerhetschefe	Under personlig uppsikt eller inlåst i rum, skåp eller liknande. Vid resa utanför EU/EES krävs godkännande av säkerhetschefen.	Under personlig uppsikt eller inlåst i säkerhetsskåp. Vid resa utanför EU/EES krävs godkännande av säkerhetschefen.

[14] Med skärm avses alla typer av elektronisk skärm på dator, läsplatta, telefon, projektor eller liknande. Observera att t.ex. trådlös överföring av skärmbilder kan vara sårbar.

		n.		
Sändning eller mottagande av e-post inom kommunen samt med godkända externa aktörer[15] (Ref.: M 8.9, M 8.15, M 8.16, M8.17)	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem. Vissa informations-typer kräver filkrypto.

Hanteringsregler – exempel på aktiviteter (situationer)	Informationsklass gällande konfidentialitet			
	0. Grön: Öppen information	1.Gul: Intern information	3.Orange: information med sekretess	4.Röd: information med stark sekretess
Sändning eller mottagande av e-post till och från övriga aktörer (Ref.: M 8.9, M 8.15, M 8.16, M8.17)	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem.	Tillåtet med kommunens e-postsystem och användning av godkänd funktion för filkrypto.
Informationsutbyte via chatt (Ref.: M 8.18)	Tillåtet via kommunens godkända tjänster.	Tillåtet via kommunens godkända tjänster.	Inte tillåtet.	Inte tillåtet.
Informationsutbyte via distansmöte (Ref.: M8.15, M8.19, M8.20)	Inga restriktioner.	Inga restriktioner.	Inga restriktioner.	Tillåtet med interna och godkända externa parter undantaget vissa informationstyper.
Hanteringsregler – exempel på aktiviteter	Informationsklass gällande konfidentialitet			

[15] För vissa externa godkända aktörer gäller särskilda regler, se kapitel 2.8 – Digital kommunikation (e-post, chatt, distansmöten).

(situationer)	0. Grön: Öppen information	1.Gul: Intern information	3.Orange: information med sekretess	4.Röd: information med stark sekretess
Pappersbrev via internpost (Ref.: M 4.11)	Inga restriktioner.	Inga restriktioner.	I förslutet kuvert till behörig mottagare.	I förslutet kuvert till behörig mottagare alternativt personlig överlämning.
Fax (Ref.: M 4.12)	Inga restriktioner.	Inga restriktioner.	Sändande och mottagande enhet ska övervakas av behörig vid överföring.	Inte tillåtet.
Distansarbete [16] (Ref.: M 6.6, M 6.8)	Endast tillåtet via kommunens godkända tjänster.	Endast tillåtet via kommunens godkända tjänster.	Endast tillåtet via kommunens godkända tjänster.	Endast tillåtet via kommunens godkända tjänster.
Destruktion av pappersdokument (Ref.: M 4.15)	Inga restriktioner. Placera dokument i papper-såtervinning.	Inga restriktioner. Placera dokument i pappers-återvinning.	Strimlas i dokumentförstöra re eller placeras i säkerhetskärl.	Strimlas i dokumentförstöra re eller placeras i säkerhetskärl.
Destruktion av datamedia[17] (Ref.: M 4.16)	Datamedia lämnas till LKDATA.	Datamedia lämnas till LKDATA.	Information raderas och datamedia lämnas till LKDATA.	Information raderas och datamedia lämnas till LKDATA.

Tabell 5. Exempel på hanteringsregler

[16] Distansarbete är ordinarie arbetsuppgifter som utförs av medarbetare på en plats som är geografiskt skild från arbetsplatsen.

[17] Med datamedia menas här hårddiskar, cd/dvd-skivor, usb-minnen och andra liknande elektroniska lagringsmedia.

Kapitel 3 - Styrning av informationssäkerhet

3.1 Inledning

För att en god informationssäkerhet ska kunna upprätthållas över tid behöver arbetet struktureras och styras. Det måste vara tydligt för kommunens medarbetare dels vilket informationssäkerhetsarbete som ska utföras i kommunen, dels vem som ska utföra det. Modeller, processer och strukturer behöver definieras för en god hantering i arbetet med informationssäkerhet. Ett system-atiskt informationssäkerhetsarbete är ett krav i standarden ISO/IEC 27000, som kommunen arbetar aktivt med att uppnå.

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Linköpings kommun. I kapitlet beskrivs den övergripande ansvarsfördelningen för informationssäkerhetsarbetet. Mer detaljerade beskrivningar för respektive målgrupp finns i kommande kapitel.

I detta kapitel förklaras även begreppet informationsklassning och kommunens modell för informationsklassning redovisas.

Den primära målgruppen för detta kapitel är personer som antingen arbetar med informations- och it-säkerhet eller ansvarar för informationssäkerhet inom kommunens olika förvaltningsobjekt och verksamheter. En sekundär målgrupp är intresserade av hur arbetet med informationssäkerhet bedrivs i kommunen.

3.2 Vilken information hanterar kommunen?

För att nå en god informationssäkerhet i en verksamhet behöver vi först identifiera vilken information som hanteras i verksamheten. Detta arbete kan utföras på många olika sätt och för en verksamhet så omfattande som Linköpings kommun är en komplett informationskartläggning ett mycket stort arbete. Kommunen har därför beslutat att använda respektive verksamhets informationshanteringsplan (IHP) som utgångspunkt, eftersom den ska innehålla de allmänna handlingar som hanteras i verksamheten.

Även information som inte är allmän handling men som ändå hanteras i verksamheten, ska informationsklassas och dokumenteras i en separat mall för arbetsmaterial. Vid de bedömningar som förklaras i kommande kapitel ska handlingar och andra informationstyper bedömas på samma sätt, oavsett om informationen är allmän eller inte. Alla informationstyper ska alltså bedömas på samma sätt. Arbetsmaterial får inte klassas lägre än hur motsvarande information klassas i en allmänna handling.

3.3 Organisation och ansvarsfördelning

För att arbetet med informationssäkerhet ska fungera bra behöver ansvaret för olika aktiviteter fördelas mellan olika befattningar inom kommunen. Det bör framgå

- vem som ansvarar för vad

- vem som beslutar om vad
- hur samarbete ska ske mellan olika roller och befattningar.

Kommande avsnitt redovisar kommunens strukturer för roller och ansvar samt hur dessa ska vara organiserade.

3.3.1 Ansvarsfördelningens grundprincip

Grundprincipen när det gäller ansvar för informationssäkerheten är att ansvaret följer det ordinarie verksamhetsansvaret hela vägen från kommunfullmäktige till enskilda medarbetare. Principen är att den som är formellt ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamheten.

För att denna grundprincip ska kunna upprätthållas och fungera behöver de ansvariga stöd i informationssäkerhetsarbetet. Detta stöd tillhandahålls främst genom denna handbok med dess bilagor, referenser och länkar samt genom olika anpassade utbildningsmaterial. Rådgör med informationssäkerhetssamordnaren gällande informationsunderlag och utbildningmaterial.

Figur 16. visar hur informationssäkerhetssamordnaren och övriga säkerhetsroller i kommunen agerar resurs och kompensationsstöd till verksamheter, chefer och medarbetare i kommunen.

Informationssäkerhetssamordnaren och övriga roller som arbetar med informationssäkerhet är tillsammans med cheferna ett resurs- och kompetensstöd för samtliga medarbetare och verksamheter i arbetet med informationssäkerhet.

Ansvarsfördelnings – grundprincip		*Fördjupad information*
●	Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret från kommunfullmäktige till den enskilda medarbetaren.	Kapitel 4.2 – Ansvar och roller

3.3.2 Övergripande ansvar

Kommunfullmäktige har det övergripande ansvaret för all kommunens säkerhet, inklusive informationssäkerhet. Det innebär att kommunfullmäktige fastställer övergripande mål och inriktning för informationssäkerheten genom en säkerhetspolicy.

Kommunstyrelsen fastställer vilka områden som ska regleras utifrån säkerhets-policyn. Denna reglering fastställs i riktlinjer för informationssäkerhet.

Kommundirektören ansvarar för att informationssäkerhetsarbetet bedrivs -enligt fastställda riktlinjer. Det sker genom den tillämpningsanvisning som -denna handbok utgör och andra styrande dokument.. Informationssäkerhets-rådet har det operativa ansvaret för att förvalta och föreslå revideringar.

Övergripande ansvarsfördelning		Fördjupad information
●	Kommunfullmäktige fastställer övergripande mål och inriktning med informationssäkerhetsarbet et.	Kommunens Säkerhetspolicy
●	Kommunstyrelsen fastställer vilka områden som ska regleras.	Kommunens riktlinje för informationssäkerhet
●	Kommundirektören fastställer tillämpningsanvisningar.	Informationssäkerhetshandboken

3.3.3 Ansvar inom respektive verksamhet

Respektive nämnd är ansvarig för informationssäkerheten inom respektive verksamhetsområde. Varje nämnds förvaltning ansvarar för verkställighet av de beslut nämnden fattar. Förvaltningar kan även besluta om -kompletterande regler och anvisningar utöver de som finns i denna handbok.

Informationssäkerhetsansvaret följer verksamhetsansvaret på samtliga nivåer inom kommunen. I varje chefsbefattning ingår ansvar för att informera personalen om reglerna i denna handbok samt se till att reglerna efterlevs. Mer information om hur detta ansvar struktureras och hanteras återfinns i kapitel 4.2 – Verksamhetsnära roller och ansvar.

Ansvaret för informationssäkerhet kan inte överlämnas. Däremot kan de arbetsuppgifter som ingår i ansvaret överlämnas, likt andra ansvarsområden inom kommunen.

Ansvar inom respektive verksamhet		Fördjupad information
●	Respektive nämnd ansvarar för informations-säkerheten inom respektive verksamhetsområde.	Kapitel 3.3 – Organisation och ansvarsfördelning Kapitel 4.3 – Chefer och verksamhetsansvariga
●	Förvaltningar ansvarar för att verkställa nämndens beslut avseende informationssäkerhet.	Kapitel 3.3 – Organisation och ansvarsfördelning Kapitel 4.3 – Chefer och verksamhetsansvariga

3.3.4 Informationsägande nämnd

En förutsättning för att information ska få ett relevant skydd är att det finns ett tydligt ansvar kopplat till informationen. Därför ska en viss typ eller en viss mängd information ha ett tydligt tilldelat ansvar. Inom Linköpings kommun är det alltid en nämnd (informationsägande nämnd) som har ansvaret för den information som hanteras i respektive verksamhet. Nämnden kan dock uppdra (överlämna) till en funktion att verkställa ansvaret. Detta uppdrag tilldelas vanligen förvaltningschefer i respektive förvaltning som rollen informationsägare.

Ansvar inom nämnd		Fördjupad information
●	Respektive nämnd ansvarar för att rollen informationsägare utses i respektive förvaltning.	Kapitel 4.4 – Informationsägare

3.3.5 Informationsägare

Informationsägarens uppgift är att fullgöra det uppdrag som överlämnats av informationsägande nämnd. Informationsägarens viktigaste uppgift är att värdera information enligt kommunens modell för informationsklassning. I uppdraget ingår också att intyga att informationen omges av skyddsåtgärder som motsvarar det önskade skyddsbehovet.

Informationsägarens ansvar att fullfölja nämndens uppdrag kan inte överlämnas; däremot kan relaterade arbetsuppgifter överlämnas till rollen informationsägarbiträde. Se även kapitel 4.4 – Informationsägare.

Ansvar som informationsägare		Fördjupad information
●	Respektive informationsägare ansvarar för att värdera respektive förvaltnings information enligt kommunens modell för informationsklassning.	Kapitel 3.7 – Informationsklassning i Linköpings kommun Kapitel 4.4 – Informationsägare
●	Respektive informationsägare är ansvarig för att löpande följa upp respektive förvaltnings efterlevnad av LIS. Resultatet av uppföljningen ska dokumenteras.	Kapitel 3.11 – Efterlevnad och granskning
●	Respektive informationsägare ansvarar för att överlämna arbetsuppgifter till informationsägarbiträde (om sådant utses).	Kapitel 4.4 – Informationsägare

3.3.6 Informationsägarbiträde

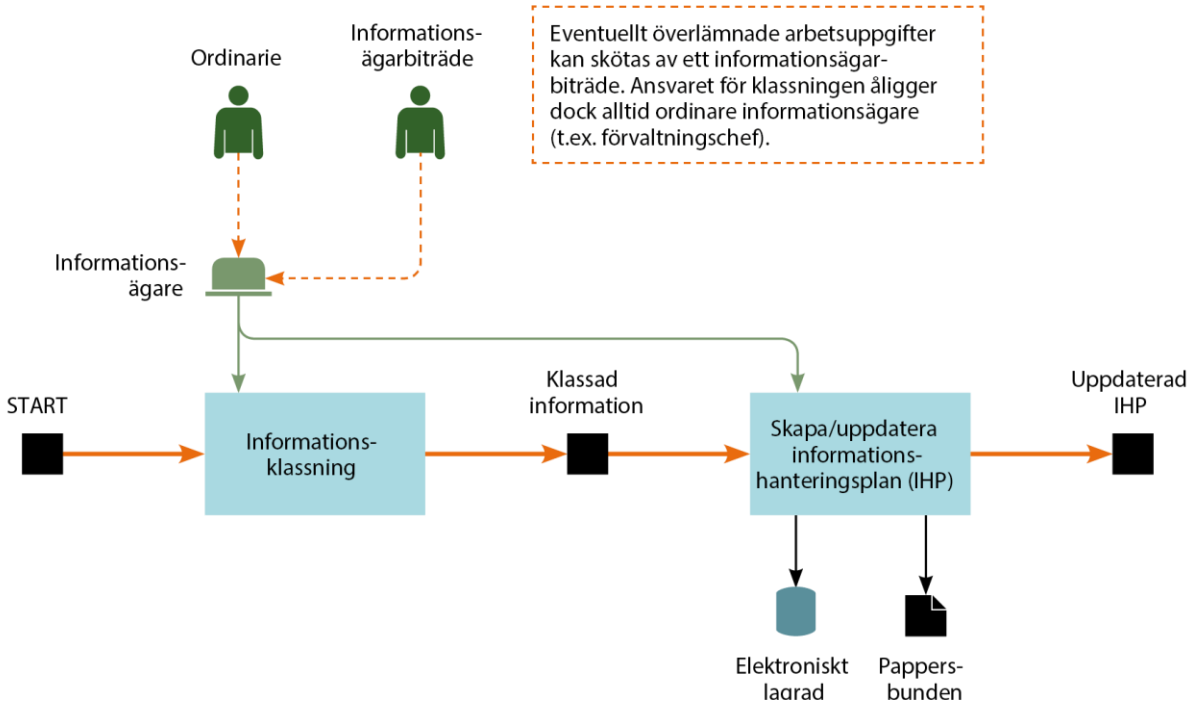
I många fall kan det vara lämpligt att informationsägaren uppdrar arbetsuppgifter till en underliggande chefsnivå som arbetar närmare den faktiska informationshanteringen. Denna

roll benämns då informationsägarbiträde och kan på uppdrag av informationsägaren utföra arbetsuppgifter som åligger informationsägaren. Syftet med detta uppdrag är att minska informationsägarens arbetsbörda och förtydliga vilka eventuella konsekvenser som kan uppstå med information.

Informationsruta

Informationsägarbiträdets kompetens

Om informationsägaren överlämnar arbetsuppgifter till ett eller flera informationsägarbiträden behöver rollen bemannas av medarbetare som har bred erfarenhet av informationshantering i verksamheten.

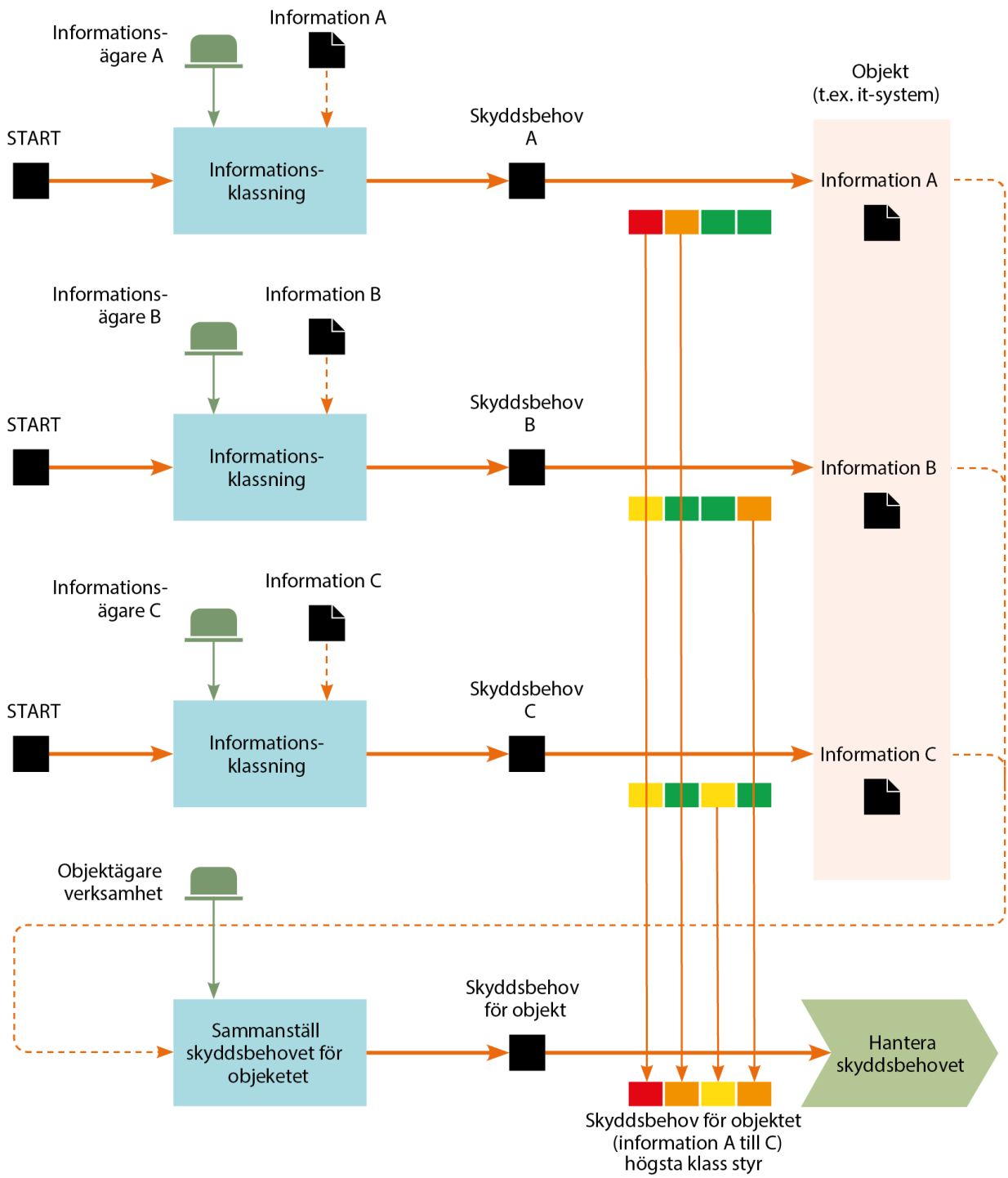


Figur 17. Fördelning av ansvar och arbetsuppgifter vid informationsklassning. Figuren visar en fördelning av ansvar och arbetsuppgiftersprocess. Där ordinarie och informationsägarbiträde är infomationsägare och ansvarar för informationsklassning samt att skapa/uppdatera IHP. Informationsklassingen blir i processkartan klassad information som sedan skapas och lagrad elektroniskt eller på papper. Därefter blir IHP uppdaterad.

Ansvar som informationsägarbiträde		Fördjupad information
●	Informationsägarbiträde ansvarar för att utföra överlämnade arbetsuppgifter från informationsägare.	Kapitel 3.7 – Informationsklassning i Linköpings kommun Kapitel 4.4 – Informationsägare

3.3.7 Objektägares ansvar

Objektägare verksamhet och objektägare it (enligt kommunens förvaltningsmodell pm3) ansvarar för att förvaltningsobjekten uppfyller de krav som ställs i denna handbok. En viktig del av detta ansvar, vilket åligger objektägare verksamhet, är att sammanställa informationsägarnas klassning av den information objektet hanterar, med andra ord objektets skyddsbehov (se kapitel 3.4 Informationssäkerhetsorganisation).



figur 18. Hur skyddsbehov vidareleds i verksamheten enligt pm3. (Figuren visar en processkarta över hur skyddsbehov vidareleds i verksamheten enligt pm3. Processkartan visar 4 stycken informationsägare med information som informationsklassas. Informationsklassningen går sedan igenom ett skyddsbehov, som sedan skapar objektsinformation, som i sin tur får en skyddsbehovssammanställning. Därefter hanteras skyddsbehovet.)

Resultatet från informationsklassningen förmedlas till den it-nära förvaltningen så att rätt skyddsåtgärder kan tilldelas de resurser/objekt som hanterar informationen. Objektägarna ansvarar för att godkänna varje it-komponent för en viss nivå av informationsklassad information som kan hanteras i it-komponenten. Informationssäkerhetsansvaret hos övriga roller beskrivs för verksamhetsnära förvaltning i kapitel 4.2 – Verksamhetsnära roller och ansvar och för it-nära förvaltning i kapitel 5.2 – It-nära roller och ansvar.

Objektägare Verksamhet ansvarar för…		Fördjupad information
●	Objektägare Verksamhet ansvarar för att ta emot berörda informationsägares skyddsbehov samt sammanställa och vidarebefordra objektens skyddsbehov.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.2 – It-nära roller och ansvar Kapitel 6.2 – Allmänt om säkerhet och fysiskt skydd
●	Objektägare Verksamhet och Objektägare it -ansvarar för att godkänna varje it-komponent för en viss nivå av informationsklassad information som kan hanteras i it-komponenten.	Kapitel 3.3.7 – Objektägares ansvar Kapitel 3.6 – Informationsklass-ningens grunder, underrubriken Förvalta.

3.3.8 Medarbetares ansvar

Varje medarbetare har ett personligt ansvar att följa kommunens regler och anvisningar så att en god informationssäkerhet kan uppnås. I kapitel 2 – Informationssäkerhet för medarbetare finns de regler och anvisningar som samtliga medarbetare ska följa; därutöver kan det även finnas kompletterande regler och anvisningar för den egna verksamheten.

Ansvar som medarbetare		Fördjupad information
●	Respektive medarbetare ansvarar för att följa kommunens regler och anvisningar.	Kapitel 2 – Informationssäkerhet för medarbetare

3.3.9 Personuppgiftsansvar

Respektive nämnd är personuppgiftsansvarig för all behandling av personuppgifter inom nämndens ansvarsområde, och varje nämnd ska ha ett dataskyddsombud som ansvarar för tillsyn och rådgivning. Kommunstyrelsen utser dataskyddsombud för samtliga nämnder.

Ansvar för personuppgifter		Fördjupad information
●	Respektive nämnd har ansvar för all behandling av personuppgifter inom nämndens ansvarsområde.	Kapitel 4.2 – Verksamhetsnära roller och ansvar
●	Chefsjuristen har delegation på att utse dataskyddsombud för samtliga nämnder.	Kapitel 2.3.4 – Informations-klassning och personuppgifter

3.3.10 Stadsarkivets ansvar

Stadsarkivet hanterar allmänna handlingar som har lämnats för bevarande samt ser till att dessa hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen samt offentlighets- och sekretesslagen. Stadsarkivet ansvarar också för kommunens interna styrdokument om hur information ska hanteras och bevaras långsiktigt.

När information arkiveras övergår informationsägarskapet till kommunstyrelsen (genom Stadsarkivet). Som stöd i denna process har Stadsarkivet tillgång till den avsändande verksamhetetens informationshanteringsplan, vilken verksamheten tagit fram i samråd med arkivet. Planen innehåller information om hur verksamheten har bedömt den aktuella informationens informationssäkerhetsaspekter (se kapitel 3.6 – Informationsklassningens grunder), och det är aspekten konfidentialitet som normalt följer med informationen in i arkivet. Därför styrs åtkomst till informationen primärt av denna klassning.

Stadsarkivet ansvarar också för att upprätta och förvalta mallen för informationshanteringsplanen.

Ansvar för stadsarkivet		Fördjupad information
●	Respektive nämnd ansvarar för att verksamhetens handlingar hanteras enligt lag. När handlingar överlämnas till Stadsarkivet överförs även ansvaret för denna hantering dit..	Kapitel 7.2.4 – Lagar och regelverk som relaterar till informationssäkerhet
●	Stadsarkivet ansvarar för att upprätta och förvalta mallen för kommunens informations-hanteringsplan (IHP).	Kapitel 3.2 – Vilken information hanterar kommunen?

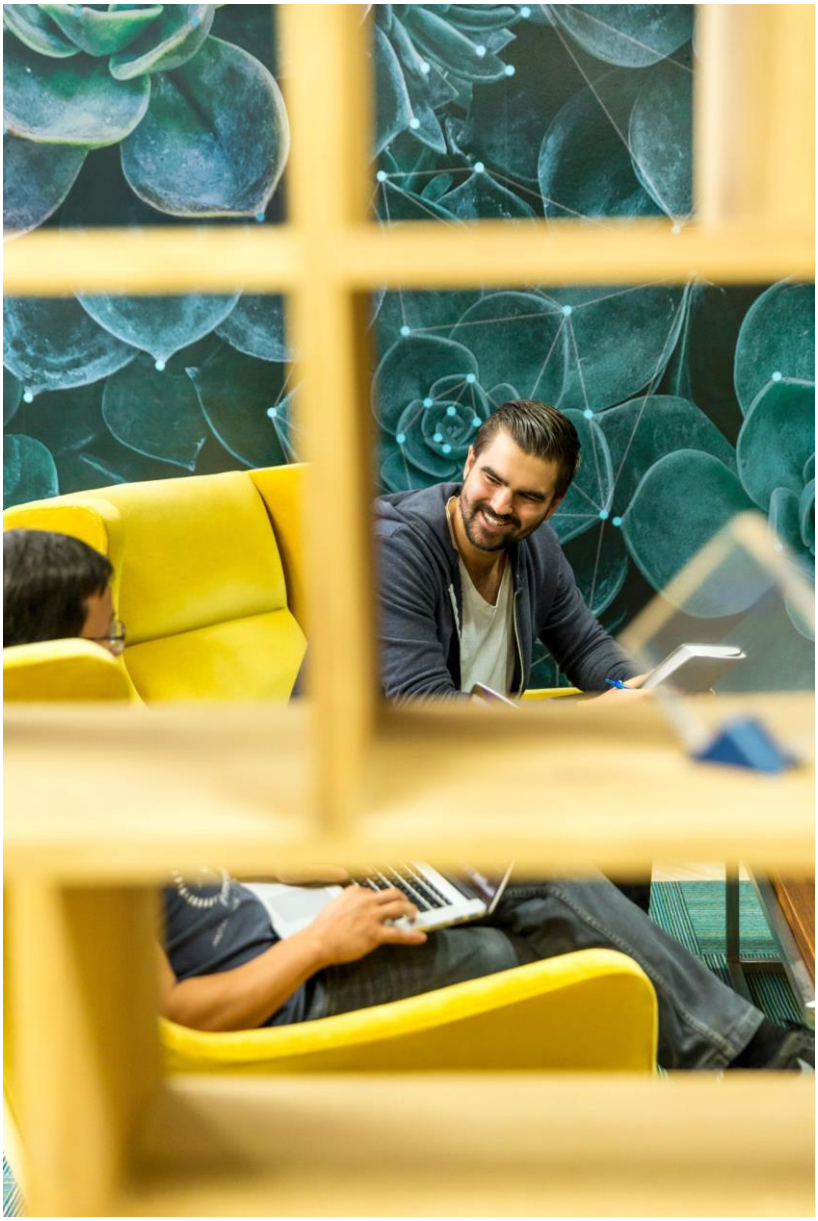


Bild: Visar två personer i en soffa. Ena personen håller bärbar dator and i ett anteckningsblock.

3.3.11 Ansvar i projekt

Ett projekt i kommunen ägs normalt av den verksamhet som initierat projektet. Verksamhetens representant i projektet har rollen som projektbeställare tillika informationsägare. Det är därför projektbeställaren ansvar att bedöma (informationsklassa) den information som ska hanteras i projektet och den tänkta information som projektet kan komma att resultera i, t.ex. nya handlingar (informationstyper). Om projektet hanterar kända handlingar (informationstyper), ska skydds--behoven härledas utifrån befintlig informationsklassning i verksamhetens informationshanteringsplan.

Tillsammans med projektets styrgrupp fastställer projektbeställare de informationssäkerhetskrav som ska gälla för projektet och för resultatet. Efter informationsklassningen ska klassningsresultatet vidimeras med de informationsägare som berörs av projektet.

Projektets styrgrupp ansvarar för att löpande bevaka att fastställda informations-säkerhetskrav implementeras och följs. Avvikelser rapporteras till projektbeställ-aren. Projektledaren ansvarar för att beslutade informationssäkerhetskrav införs och efterlevs i projektet. Projektledaren rapporterar till projektets styrgrupp. När projektet avslutas ska alla kvarvarande avvikelser rapporteras till berörda objekt-ägare verksamhet och objektägare it.

Ansvar för stadsarkivet		Fördjupad information
●	Projektbeställaren ansvarar för att informations-klassning sker av den information som hanteras i projektet.	Kapitel 4.7 – Informationsklassning
●	Projektbeställaren ansvarar för att fastställa projektets informationssäkerhetskrav och vidimera dessa med berörda informationsägare.	Kapitel 5.9 – Anskaffning och utveckling av it-komponenter Kapitel 5.10 – Informations-säkerhetskrav vid upphandling
●	Projektets styrgrupp ansvarar för att fastställda informationssäkerhetskrav efterföljs samt att rapportera avvikelser till projektbeställare.	Kapitel 5.9 – Anskaffning och utveckling av it-komponenter Kapitel 5.10 – Informations-säkerhetskrav vid upphandling
●	Projektledaren ansvarar för att beslutade skyddsåtgärder införs.	Kapitel 5.9 – Anskaffning och utveckling av it-komponenter Kapitel 5.10 – Informations-säkerhetskrav vid upphandling

3.3.12 Ansvar vid samverkansaktiviteter

Linköpings kommun samverkar ofta med andra aktörer, t.ex. andra kommuner, myndigheter samt offentliga eller privata organisationer. Dessa samverkansaktiviteter hanterar och utbyter ofta information i olika forum, främst via digitala plattformar.

Medarbetare i kommunen får inte starta samarbeten i andra plattformar än de som tillhandahålls av Linköpings kommun.

Medarbetare får medverka i samarbeten med andra myndigheter via deras platt-formar om man har gjort en sekretessprövning som medger att informationen kan lämnas ut. Efter utlämning är det den myndighet som äger plattformen som ansvarar säkerheten i hanteringen.

För privata aktörer gäller ovanstående under förutsättning att aktören ifråga har samma legala krav på sekretess och tystnadsplikt som kommunen. I annat fall kan enbart information ur informationsklass 0 och 1 överföras. Om ytterligare information behöver överföras kan förfrågan ställas till informationssäkerhetsrådet som bereder den för beslut av informationsägaren.

Ansvaret för informationssäkerhet vid samverkansaktiviteter hanteras likt ansvaret i projekt, och en informationsägare ska utses för den information som hanteras inom aktiviteten. Detta gäller oavsett vem som initierat aktiviteten – någon utanför kommunen eller kommunens medarbetare. Det kan även vara lämpligt att utse ett informationsägarbiträde som hanterar informationen i forumet och ser till att beslutade krav följs.

Om kraven på informationshantering redan är kända eller kan härledas från t.ex. befintliga informationshanteringsplaner kan det vara tillräckligt att utse ett informationsägarbiträde för den löpande förvaltningen av forumet.

Ansvar för stadsarkivet		Fördjupad information
●	Den medarbetare som initierat samarbets-aktiviteten ansvarar för att ett informations-ägarbiträde utses som hanterar informationen i forumet.	Kapitel 4.7 – Informationsklassning

3.4 Informationssäkerhetsorganisation

Kommunen har ett antal roller rörande informationssäkerhet.

3.4.1 Informationssäkerhetssamordnaren

Kommunens informationssäkerhetsarbete ska samordnas av en informationssäkerhetssamordnare och rapportering sker till säkerhetschefen. Förändrade eller kompletterande regler eller avsteg från regler och anvisningar i denna handbok bereds av samordnaren, behandlas i informationssäkerhetsrådet och beslutas av kommundirektören.

Informationssäkerhetssamordnaren ansvarar för att		Fördjupad information
●	analysera kommunens hotbild, skyddsnivå samt interna och externa krav inom informationssäkerhetsområdet	Kapitel 3.6 – Informationsklas-sningens grunder
●	föreslå revideringar av kommunens styrande dokument inom området, t.ex. Riktlinjer för informationssäkerhet och Informationssäkerhetshandbok en.	Kapitel 3.5 – Kommunens centrala dokument för styrning
●	utveckla och förvalta metoder, vägledningar, skyddsbehov och annat stödmaterial inom informationssäkerhetsområdet.	Informationssäkerhetshandbok för Linköpings kommun
●	öka informationssäkerhetsmedveta ndet inom kommunen, t.ex. genom rådgivning, utbildning och andra kompetenshöjande åtgärder samt stöd till verksamheterna i frågor som rör informationssäkerhet	Informationssäkerhetshandbok för Linköpings kommun
●	kontrollera och följa upp arbetet med informationssäkerhet	Kapitel 3.11 – Efterlevnad och granskning
●	ha kontroll över verksamheters godkända avsteg från regler och anvisningar i denna handbok	Kapitel 3.12 – Dispenser och undantag från handboken
●	bedriva omvärldsbevakning inom informationssäkerhetsområdet	
●	sammanställa kommunens identifierade informationssäkerhetsrisker	Kapitel 4.8 – Analys och hantering av risker
●	leda kommunens informationssäkerhetsråd	Kapitel 3.4.3 – Informations-säkerhetsrådet

3.4.2 It-säkerhetssamordnaren

It-säkerhetssamordnaren koordinerar arbetet med informationssäkerhet i den it-nära verksamheten (LKDATA) och kan bl.a. bistå som stöd vid kravställning på externa aktörer. Rollen it-säkerhetssamordnare beskrivs mer utförligt i kapitel 5.2 – It-nära roller och ansvar.

3.4.3 Informationssäkerhetsrådet

I Linköpings kommun finns ett informationssäkerhetsråd som behandlar informationssäkerhetsrelaterade ärenden. Informationssäkerhetsrådet består av kommunens säkerhetschef, CIO, it-säkerhetssamordnaren, objektägare it, informationssäkerhetssamordnaren samt chefsjurist som även leder forumet och adjungerar övriga medlemmar (t.ex. företrädare för juridik, fastigheter och digitalisering) efter behov beroende på aktuella ärendens art.

Informationssäkerhetsrådet ansvarar för att		Fördjupad information
●	registrera och bereda ärenden som gäller undantag från kommunens handbok	Kapitel 3.12 – Dispenser och undantag från handboken
●	bereda förändringar av informationssäkerhetshandbokens innehåll	Kapitel 3.5 – Kommunens centrala dokument för styrning
●	bereda dokument, t.ex. styrande dokument, metoder, verksamhetskrav och vägledningar	Kapitel 3.5 – Kommunens centrala dokument för styrning
●	fungera som remissinstans och rådgivare i frågor som berör informationssäkerhet för att säkerställa följsamhet med kommunens LIS	Kapitel 3.3.1 – Ansvars-fördelningens grundprincip
●	vara ett forum för erfarenhetsutbyte och omvärldsbevakning	
●	genomföra uppföljning av informationssäkerhetsincidenter och initiera säkerhetshöjande åtgärder	Kapitel 5.11 – Incidenthantering
●	genomföra riskuppföljning och initiera riskmitigering	Kapitel 4.8 – Analys och hantering av risker
●	fastställa arbetssätt och stödjande information för informationsäkerhetsarbetet	Kapitel 5 – Informationssäkerhet i it-nära förvaltning

●	samråda med dataskyddsombuden	Kapitel 3.3.9 – Personuppgifts-ansvar
●	följa upp regelverkets och säkerhetsorganisationens ändamålsenlighet	Kapitel 3.11 – Efterlevnad och granskning

ID	Regler och anvisningar för informationssäkerhetsorganisation
S 4.1 0 1 2 3	Kommunens informationssäkerhetsarbete ska samordnas av en informationssäkerhetssamordnare som rapporterar till säkerhetschefen.
S 4.2 0 1 2 3	En it-säkerhetssamordare ska samverka med informationssäkerhetssamordnaren i frågor som rör den it-nära verksamheten.
S 4.3 0 1 2 3	Ett informationssäkerhetsråd ska finnas för att behandla informationssäkerhetsrelaterade ärenden i kommunen.

3.5 Andra dokument med betydelse för informationssäkerhet

Risk- och sårbarhetsanalys (RSA) är en analys av extraordinära händelser som kan inträffa inom kommunens geografiska områdesansvar. Den ska enligt- lag utföras vart fjärde år. I RSA kan det förekomma risker och sårbarheter som har en koppling till informationssäkerhet. Kommunens RSA kan därför i viss mån sägas komplettera arbetet med informationssäkerhet och utfallet av RSA och säkerhetsskyddsanalys kan ha en påverkan på informationssäkerhetsanalysen. I de delar det rör sig om hot eller risk för hot mot kommunens informationssäkerhet och det antas ha en påverkan på Sveriges säkerhet, ska dessa istället hanteras i kommunens säkerhetsskyddsanalys.

Informationssäkerhetsanalys intern verksamhet innehåller en genomlysning av informationssäkerheten i Linköpings kommun vad gäller hotbild, skyddsnivåer, kommunens inriktning samt interna och externa krav. Analysen genomförs i full skala vart fjärde år men justeringar görs löpande vid förändringar inom kommunen eller externt. Informationssäkerhetsanalysen ligger till grund för arbetet med informationssäkerhet, vilket kan påverka innehåll och utformning av övriga styrande dokument. Dokumentet upprättas av informationssäkerhetssamordnaren.

Handlingsplan för informationssäkerhet tas fram årligen av informationssäkerhetssamordnaren utifrån en informationssäkerhetsanalys av intern verksamhet samt kommunens RSA och innehåller konkreta mål och åtgärder. Dokumentet upprättas av informationssäkerhetssamordnaren och säkerhetschefen.

Informationssäkerhetssamordnaren ansvarar för att ta fram modeller, metoder, vägledningar och andra stöddokument som dels stödjer arbetet med informationssäkerhet på olika nivåer,

dels underlättar tillämpning och efterlevnad av säkerhetspolicyn, riktlinjerna och handboken för informationssäkerhet.

Ytterligare ett antal dokument påverkar kommunens informationshantering. Dessa finns att läsa på Linweb:

- Linköpings kommuns reglemente
- Handbok för digital arkivering
- Ärendehandboken
- Pm3 förvaltningsstyrningsmodell.

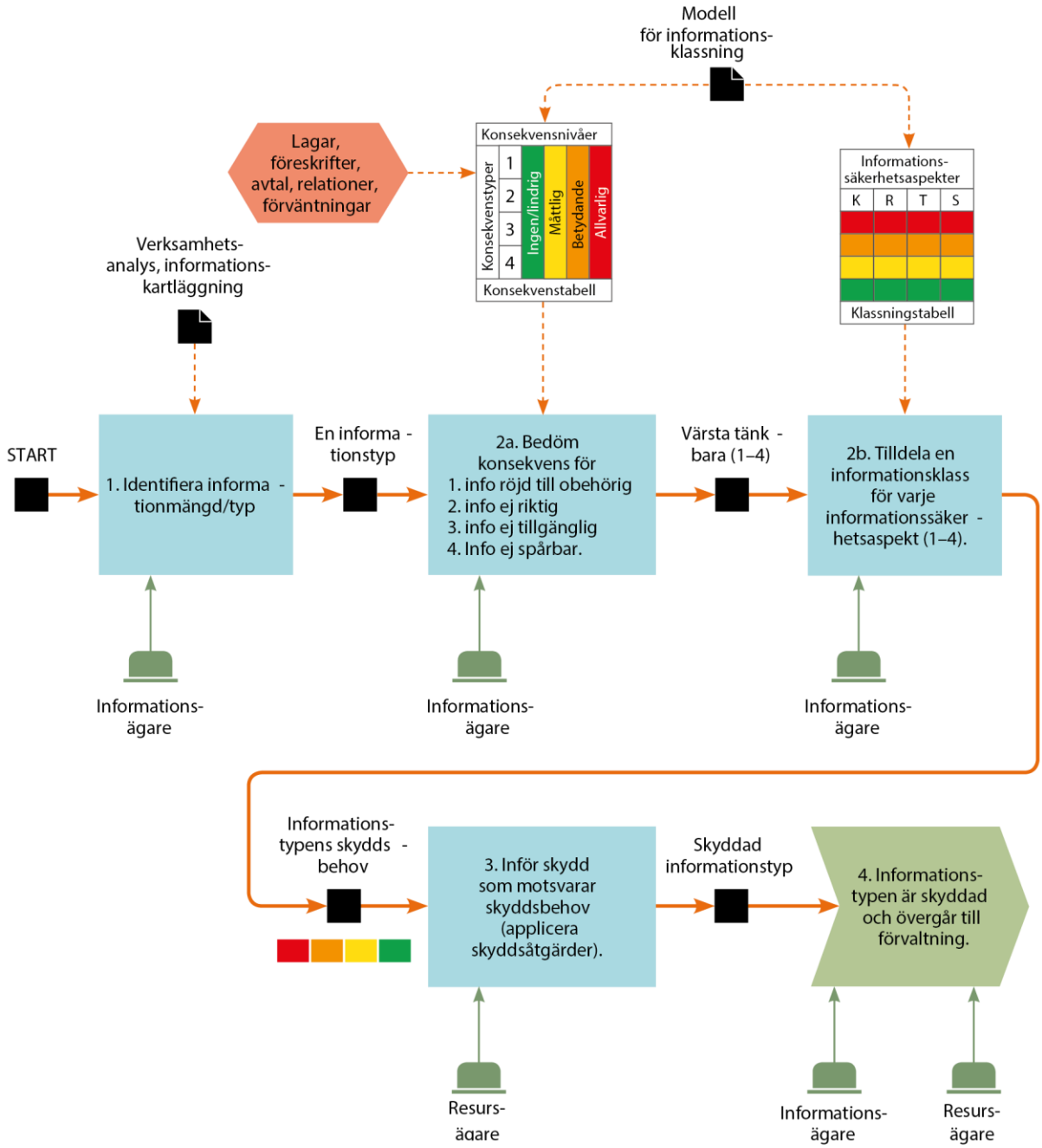
Lokalt i de olika verksamheterna kan mer specifika instruktioner och vägledningar tas ofta fram med stöd av informationssäkerhetssamordnaren, i syfte att komplettera och förtydliga kraven i denna handbok.

ID	Regler och anvisningar för dokumentstruktur för informationssäkerhet
S 5.1	Risker och sårbarheter som berör informationssäkerhet som identifieras i en risk- och sårbarhetsanalys (RSA) eller en informationssäkerhets-analys för intern verksamhet ska beaktas i arbetet med informationssäkerhet.
S 5.2	Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på kommunens RSA och informationssäkerhetsanalysen för intern verksamhet.
S 5.3	Modeller, metoder, vägledningar och andra stöddokument ska finnas. Dessa ska öka olika gruppers möjlighet att följa informationssäkerhetpolicyn, riktlinjerna för informationssäkerhet och informationssäkerhetshandboken.

3.6 Informationsklassningens grunder

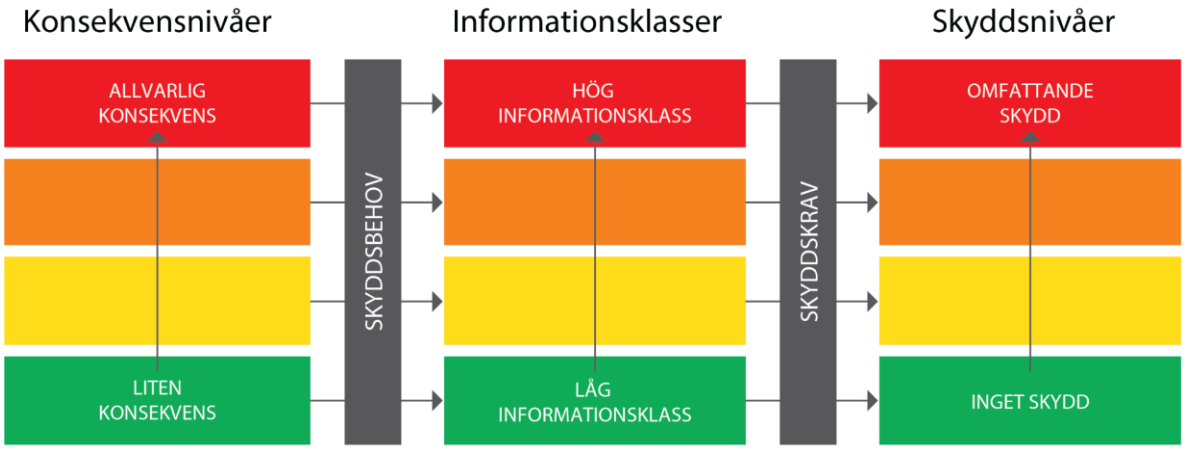
Syftet med informationsklassning är att information i en verksamhet ska förses med ett lämpligt och tillräckligt skydd. All information är inte lika värdefull, och därför kommer skyddet att variera både i omfattning och styrka. Därför används begreppet lämplighet, eftersom skyddet knyts till informationens värde för verksamheten.

Förenklat kan processen informationsklassning utryckas i fyra huvudsakliga steg, inkluderat fördelning av ansvar, enligt figur 25 nedan.



Figur 19. Informationsklassningens fyra steg. Denna figur visar en processkarta kring informationsklassingens fyra steg. Dessa fyra steg förklaras mer utförligt i texten nedan.

Steg 1. Identifiera
I denna process identifieras verksamhetens informationstyper. Informationsägaren ansvarar för denna process men vanligen inkluderas även medarbetare med erfarenhet från informationshantering i den aktuella verksamheten.
Steg 2. Bedöma
Under klassningen bedöms hur allvarligt en skada påverkar verksamheten. Graden av påverkan benämns med ett sammanfattande begrepp som konsekvensen för verksamheten. Här förutsätts att verksamheten tillämpar en metod med informationssäkerhetsaspekter, skyddsnivåer, konsekvensnivåer och konsekvenstyper, stödjande tabeller samt hur olika skador på verksamhetenska bedömas vid en informationsskada. Enligt metoden värderas (klassas) informationstypen genom att värsta möjliga konsekvens (utifrån tillämpad metod) för respektive informationssäkerhetsaspekt identifieras. Informationsägaren ansvarar för denna process men även medarbetare med vana av informationshantering samt erfarenhet från att bedöma skador kan med fördel inkluderas.



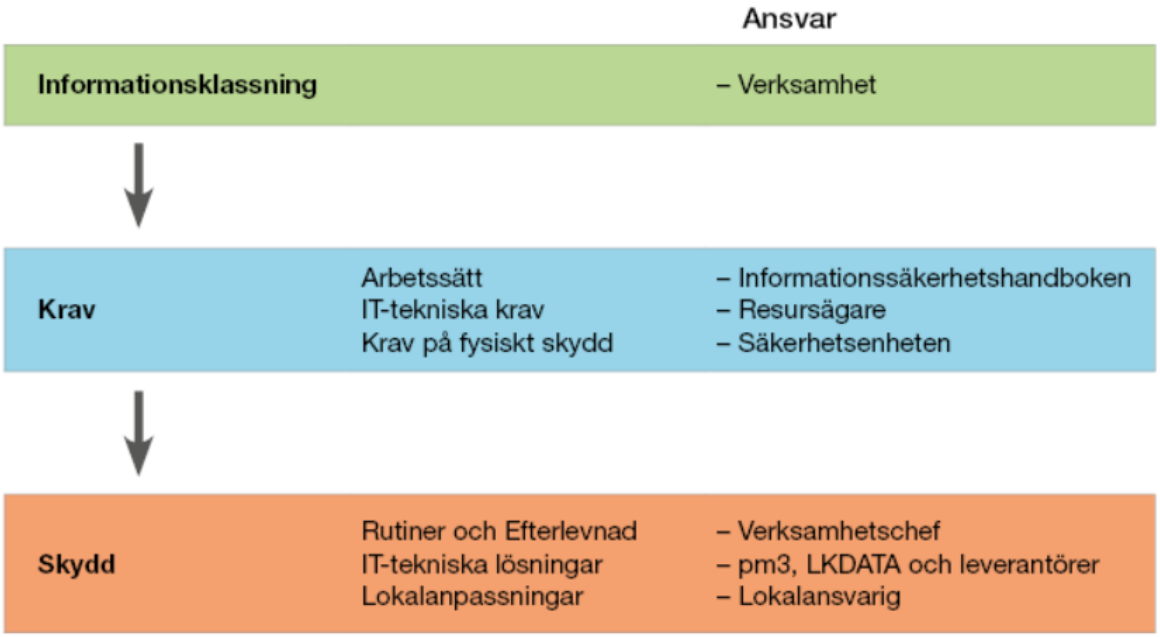
Figur 20. Exempeltabell som visar att konsekvenser leder till behov av skydd. Figuren visar en tabell med tre rubriker. Konsekvensnivåer, Informationsklasser och Skyddsnivåer. Varje rubrikstabell följs utav 4 färgrutor. Grön, gul, orange och röd. Där grön betyder liten eller låg konsekvens och röd hög/allvarlig. Mellan rubriken konsekvensnivåer och informationsklasser finns en skyddsbehovs ruta, och mellan informationsklasser och skyddsnivåer finns en skyddskravsruta.

Resultaten från bedömningen av konsekvenser skapar informationstypens informationsklass för respektive informationssäkerhetsaspekt. De fyra informationssäkerhetsaspekterna tillsammans beskriver informationstypens skyddsbehov.

Steg 3. Inför skydd
Utifrån informationsklassningen ställs fördefinierade krav på skyddsåtgärder inom tre områden.

- Krav på arbetssätt ställs i den här handboken och kompletterande rutiner.
- Krav på it-tekniska skyddsåtgärder ställs av resursägaren, vanligen CIO
- Krav på fysiska skyddsåtgärder ställs av Säkerhetsenheten.

Avvikelser mot de skyddsåtgärder som föreskrivs kan hanteras som risker -genom riskanalys och beslut om accepterad risk av behörig riskägare.



Figur 21. Informationens klassning leder till krav på skyddsåtgärder. Figuren visar de tre områdena på rad. De olika områdena förklaras i texten ovan.

Om en resurs hanterar flera typer av information är det respektive högsta klassning från respektive informationssäkerhetsaspekt som ger resursen dess skyddsbehov.

Informationstyper	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
Ärende	2	2	2	1
Beslut	0	3	2	3
Webb text	0	2	2	1
Faktura	0	3	1	2
Systemets skyddsbehov	2	3	2	3

Figur 22. Visar en tabell över ett it-systems sammanlagda skyddsbehov fås genom att leta upp det högsta värdet inom varje aspekt från alla informationstyper som hanteras av it-systemet.

Det är resursägaren som ansvarar för att applicera skyddsåtgärder i linje med skyddsbehovet. I de fall skyddsbehovet och förmågan att skydda inte stämmer överens, ska detta återrapporteras som en risk till samtliga berörda informationsägare.

Steg 4. Förvalta
Resursägaren har ansvaret för att de skyddsåtgärder som har valts också upprätthålls över tid. Om skyddet inte kan upprätthållas för en resurs ska detta rapporteras till berörda informationsägare. Andra informationssäkerhetsroller i verksamheten deltar också i arbetet löpande, så att skyddet överensstämmer med de faktiska skyddsåtgärderna. Varje pm3 objekt ska ajourhålla en förteckning över vilken skyddsnivå olika it-komponenter är anpassade för. Förteckningen anger vilka informationsklasser som it-komponenten är godkänd för att hantera.

3.7 Informationsklassning i Linköpings kommun

Utgångpunkten för informationsklassning är de handlingstyper som anges i respektive verksamhets informationshanteringsplan (IHP), där en handlingstyp motsvaras av en avskild mängd information (informationstyp) som en verksamhet har valt att identifiera och hantera specifikt.

Informationsklassningen ska göras inom varje verksamhet och informationsägaren ansvarar för att klassningen utförs och dokumenteras i verksamhetens IHP. Arbetet görs bäst av en liten grupp personer som är väl insatt i den verksamhet vars information bedöms. Gruppen behöver också förstå vilka konsekvenser det får för verksamheten och individer om information påverkas.

Det är dock viktigt att konsekvenser varken underskattas eller överskattas eftersom detta kan leda till att fel skydd väljs, vilket i sin tur kan innebära onödiga risker eller omotiverade kostnader.

Klassningen ska revideras om någon större förändring skett som kan påverka klassningens resultat.

Vid informationsklassningen bedömer informationsägaren och verksamhetskunniga medarbetare endast eventuella konsekvenser om information blir röjd, inte är riktig, inte är spårbar eller inte är tillgänglig. Genom att beskriva vad som skulle kunna hända kan informationens skyddsbehov bedömas utan att man behöver bedöma vare sig sannolikheten att det sker eller hur informationen är skyddad i dag.

Informationsruta
Viktigt att komma ihåg om klassningen
Den grupp som under ledning av informationsägaren (eller informationsägarbiträdet) utför klassningen ska endast fokusera på att bedöma konsekvenser. Diskutera eller involvera aldrig vilket skydd som krävs eller inte – denna bedömning ligger helt utanför klassningen och detta ansvar åligger inte informationsägaren.

De roller, funktioner och enheter som ansvarar för de resurser där den klassade informationen hanteras ska även se till att rätt skyddsåtgärder är implementerade.

För verksamheten i sig är det chefer som ansvarar för att medarbetarna hanterar den klassade informationen korrekt, dvs. följer regler och anvisningar i denna handbok. För it-tjänster är det objektägare verksamhet tillsammans med objektägare it som ansvarar för att rätt skyddsåtgärder finns implementerade, kopplat till den information it-tjänsten hanterar. Observera att verksamheterna också är ansvariga för att tillgodose skyddsbehovet för det fysiska skyddet, eftersom även det skyddet ska appliceras inom verksamheten.

3.7.1 Kommunens modell för informationsklassning

Linköpings kommun klassar informationstyper i fem informationsklasser som är kopplade till konsekvensnivåer. Bedömningen görs i fyra informationssäkerhetsaspekter. Informationsklassning leder till krav på skyddsåtgärder i fem skyddsnivåer.

Konfidentialitet är den vanligaste informationssäkerhetsaspekten i det dagliga -arbetet. Därför har varje nivå av konfidentialitet en egen benämning (markerad med fetstil i tabellen). Det finns inga motsvarande benämningar för aspekterna riktig-het, tillgänglighet eller spårbarhet. Dessa informationssäkerhetsaspekter kommer endast benämnas med sin korrelerande skyddsnivå, exempelvis att skyddsbehovet för informationstypen är tillgänglighet 3, riktighet 2 och spårbarhet 2.-

Skydds-nivå	Informationssäkerhetsaspekter			
	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
4 Svart: Mycket högt skydds-behov	Säkerhetsskydds-klassficerad Säkerhetsskydds-klassificerade upp-gifter. Information som rör Sveriges säkerhet.	Information som om den inte är riktig och fullständig medför synnerligen allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktör-er eller medborgare.	Information eller funktion som om den inte är tillgänglig medför synnerligen allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför synnerlig-en allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
3 Röd: Högt skydds-behov	Information med Stark sekretess -som innehåller uppgift som omfattas av -stark eller absolut sekretess eller uppgift som hänför sig till 18 kap OSL, eller en mycket stor mängd känsliga -personuppgifter som inte omfattas av stark eller absolut sekretess, där spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.	Information som om den inte är riktig och fullständig medför allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivit-et som om den inte är spårbar medför allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
2 Orange:	Sekretess Information som	Information som om den inte är	Information eller funktion som om	Information eller aktivit-et som om den

Förhöjt skydds-behov	om-fattas av svag sekretess enligt OSL eller känsliga personuppgifter enligt GDPR, där spridning kan medföra betyd-ande konsekvenser för kommunen eller annan part.	riktig och fullständig medför betydande konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	den inte är tillgänglig medför betyd-ande konsekvens för kommunen eller annan part, t.ex. externa aktör-er eller medborgare.	inte är spårbar medför betyd-ande konsekvens för kommunen eller annan part, t.ex. externa aktör-er eller medborgare.
1 Gul: Grund-läggand e skydds-behov	Intern Information som är avsedd att och utan -konsekvenser kan spridas till medarbet-are inom Linköpings kommun och till externa aktörer som be-höver informationen.	Information som om den inte är riktig och fullständig medför måttlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion- som om den inte är tillgänglig medför måttlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller aktivit-et som om den inte är spårbar medför måttlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
0 Grön: Inget skydds-behov	Öppen Information som är avsedd att och utan konsekvenser kan spridas fritt inom och utom Linköpings kommun.	Information som om den inte är riktig och fullständig medför ingen eller lindrig -konsekvens för kommunen eller annan part, t.ex. externa akt-örer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför ingen eller lindrig konsekvens för kommunen eller annan part, t.ex. externa akt-örer eller medborgare.	Information eller aktivitet som om den inte är spårbar medför ingen eller lindrig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.

Tabell 6. Linköpings kommuns modell för informationsklassning.

3.7.2 Skyddsnivå

Observera att den lägsta skyddsnivån (0 – grön) representerar öppen information som inte behöver något skydd mot insyn och som normalt inte har begräns-ad åtkomst. Däremot är det viktigt att förstå att all information, alltså även

öppen information, kan ha skyddsbehov när det gäller riktighet, tillgänglighet och spårbarhet. Det är dock ovanligt att en informationstyp helt saknar skyddsbehov för riktighet och tillgänglighet.

3.7.3 Konsekvensbedömning

När man ska bedöma konsekvenser är arbetet alltid enklare att utföra om man kan relatera konsekvensen till ett specifikt område eller en specifik typ – ett -konsekvensområde. Om information inte är tillgänglig när den behövs kan det uppstå behov av kostsamma reservrutiner, dvs. en ekonomisk konsekvens. Ett fel i ett it-system kan resultera i att utbetalningar av ekonomiska stöd förhindras, vilket i sin tur kan få konsekvenser för enskilda medborgare – dvs. en påverkan för individen. Bedömningar inom området konfidentialitet görs enbart efter vilka juridiska konsekvenser ett röjande innebär.

För att kunna värdera konsekvensen för en viss informationstyp behövs därför ett hjälpmedel i form av en konsekvenstabell för den del av verksamheten som påverkas, dvs. hur och var i verksamheten konsekvensen uppträder. Olika konsekvens-nivåer listas i tabell 6. I tabellens celler anges bedömningskriterier för respektive konsekvensnivå.

Informationsruta

Konsekvenserna ska bedömas kommunövergripande
Var uppmärksam på i vilken kontext konsekvenserna i tabell 6 bedöms. I samtliga områden ska konsekvenser bedömas ur kommunens perspektiv. Detta gäller oavsett nivå i verksamheten där informationsklassningen utförs. Om kontexten tillämpas felaktigt finns annars en risk för avvikelser mellan förvaltningar, trots att skyddbehovet egentligen är detsamma. Det tydligaste exemplet på detta är vid bedömning av ekonomiska konsekvenser, där exempelvis en kostnad på 100 000 kronor kan värderas som allvarlig i en verksamhet medan den bedöms som obetydlig i en annan. Sök stöd hos informationssäkerhetssamordnaren om du behöver hjälp att tillämpa konsekvenstabellen korrekt vid klassningen.

Gränsen mellan informationsklass 0 och 1 avseende konfidentialitet bygger på om informationen är avsedd att spridas. T.ex informationsmaterial på Linweb avsett för personal respektive informationsmaterial för allmänheten på den publika hemsidan.

Gränsen mellan informationsklass 2 och 3 avseende konfidentialitet, bygger på definitionerna av svag respektive stark och absolut sekretess i offentlighets- och sekretesslagen (OSL). I OSL regleras vilken sekretess som gäller för olika upp-gifter eller verksamheter. I informationsklass 2 ska sådan information klassas som omfattas av svag sekretess. I klass 3 ska sådan information klassas som omfattas av stark eller absolut sekretess eller som återfinns i 18 kapitlet OSL.

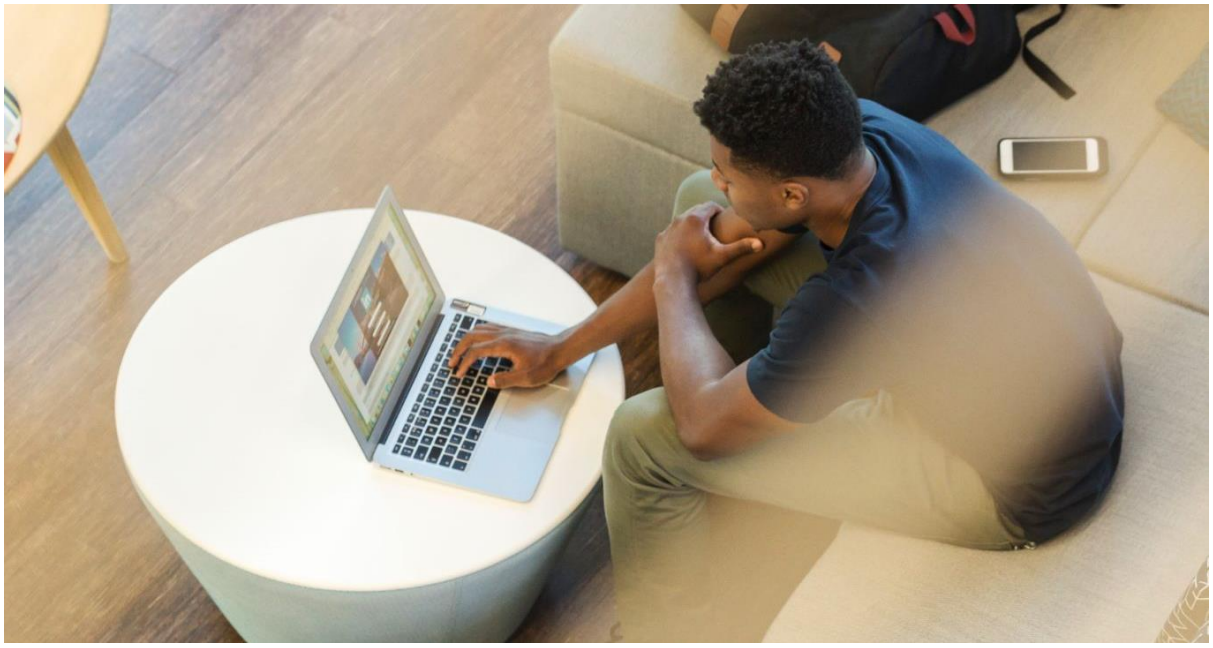


Bild: Bilden ovan visar en kille som sitter på en soffa med en bärbar dator på ett bord.

För att förstå skillnaden mellan informationsklass 2 och 3 behöver man beakta OSL:s regler för utlämnande trots att inget utlämnande ska göras.

Svag sekretess innebär att informationen som utgångspunkt är offentlig. Informationen får endast sekretessbeläggas om det kan antas att viss skada eller visst men kan uppstå. Svag sekretess indikerar att informationen vanligen kan lämnas ut om någon begär det. Endast om man av någon särskild anledning har skäl att anta att skada eller men skulle kunna uppstå, får uppgiften hemlighållas. Trots att informationen skulle komma att lämnas ut vid en begäran om allmän handling, så får kommunen inte aktivt sprida den på exempelvis kommunens hemsida, eller i övrigt hantera den på ett bristfälligt sätt. Svag sekretess kan exempelvis gälla för de avtal som kommunen tecknat med olika leverantörer eller för delar av skolans verksamhet. Stark sekretess innebär att informationen som utgångspunkt är sekretessbelagd. Informationen får endast lämnas ut om det står klart att så kan ske utan att någon lider skada eller men.

Stark sekretess innebär att informationen i de allra flesta fall måste hållas hemlig. Enbart när det står klart att ett utlämnande kan göras utan att någon lider skada eller men, får uppgiften lämnas ut. Stark sekretess råder bland annat inom förskolan, hälso- och sjukvården samt inom socialtjänsten (förutom inom familjerådgivningen där det råder absolut sekretess).

Absolut sekretess innebär att informationen alltid omfattas av sekretess. Informationen får inte under några omständigheter lämnas ut till andra än de anställda som behöver uppgifterna för att kunna utföra sitt arbete. Detta gäller exempelvis för uppgifter inom familjerådgivningen eller för uppgifter som har inhämtats av kommunens växeltelefonister.

Notera att ett utlämnande av en allmän handling, som skett efter att någon begärt ut handlingen, inte ändrar informationens informationssäkerhetsklassning. Ett exempel: Patientjournaler omfattas av stark sekretess (dvs informationsklass 3). Om en patientjournal

efter en menprövning har kunnat lämnas ut till den som begärt att få ta del av den (t.ex. till patienten själv), så omfattas patientjournalen fortfarande av stark sekretess och ska förbli klassad i informationsklass 3. Även i de fall informationen kan spridas till externa aktörer som kommunen har någon form av relation till, sker det utan att själva klassningen förändras. Om den externa aktören lyder under egen lagstiftning gäller dessa regler, annars ska den externa aktören hantera informationen enligt kommunens regler och anvisningar.

3.7.4 Kommunens konsekvenstabell

De sju konsekvensområdena i tabellen är gemensamma för hela kommunen. Notera att synnerlig allvarlig konsekvensnivå inte finns med i tabellen, eftersom den endast gäller en mycket liten mängd information som rör Sveriges säkerhet.

Konsekvens-område	Konsekvensnivå			
	0 Grön Lindriga Konsekvenser kan resultera i:	1 Gul Måttliga Konsekvenser kan resultera i:	2 Orange Betydande Konsekvenser kan resultera i:	3 Röd Allvarliga Konsekvenser kan resultera i:
Juridiska konsekvenser för bedömning av Konfidentialitet.	Information som utan konsekvenser kan spridas fritt inom och utom Linköpings kommun.	Information som utan konsekvens-er kan spridas till medarbetare inom Linköpings kommun och till externa akt-örer som behöver informationen.	Information som omfattas av svag sekretess enligt OSL eller känsliga personuppgifter enligt GDPR, där spridning kan medföra betydande konsekvenser för kommunen eller annan part.	Information som innehåller uppgift som omfattas av stark eller absolut sekretess eller uppgift som hänför sig till 18 kap OSL, eller en mycket stor mängd känsliga personuppgifter som inte omfattas av stark eller absolut sekretess, där felaktig spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.
Juridiska konsekvenser för bedömning av Riktighet, Tillgänglighet och Spårbarhet	Inget brott mot lag, förordning eller avtal.	Bristande uppfyllelse av lag, förordning eller avtal, kritik eller föreläggande från tillsynsnsmyndighet, tvist.	Brott mot lag, förordning eller avtal, kan leda till rättsprocess, kritik eller föreläggande vid vite från tillsynsmyndighet.	Brott mot lag, förordning eller avtal, leder till omfattande rätts-process, allvarlig kritik eller före---lägg-ande vid vite från tillsynsmyndighet, sanktioner/ skadestånd.
Verksamhetens förmåga att utföra sin uppgift	Obetydliga avbrott i verksamheten med minimal påverkan på förmågan att	Mindre avbrott i verksamheten med begränsad påverk-an på	Betydande avbrott i verksamheten med tydlig påverkan på förmågan att lösa	Allvarliga avbrott i verksamheten där förmågan att lösa uppgiften upphör.

	lösa uppgiften.	förmågan att lösa uppgiften.	uppgiften.	
Ekonomi	Inga eller obetyd-liga ekonomiska förluster/kostnader.	Begränsade ekonomiska förluster/kostnader (mindre än 50 000 kronor).	Betydande ekonomiska förluster/kostnader (mellan 50 000 kronor och 1 miljon kronor).	Allvarliga ekonomiska förluster/kostnader (över än 1 miljon kronor).
Påverkan på individ	Ingen eller obetydlig negativ påverk-an på en enskild individs rättigheter eller hälsa.	Begränsad negativ påverkan på en enskild individs rättigheter eller hälsa.	Betydande negativ påverkan på en enskild individs rättigheter eller hälsa.	Allvarlig påverkan på en enskild individs rättigheter eller hälsa.
Påverkan på externa intressenter	Ingen eller obetydlig negativ påverkan på externa intress-enter.	Begränsad negativ påverkan på externa intressenter.	Betydande påverk-an på externa intressenter.	Allvarlig påverkan på externa intressenter.
Förtroende	Ingen eller obetyd-lig påverkan på förtroende från medarbetare eller allmänheten.	Begränsad och kortvarig påverkan på förtroende från medarbetare eller allmänheten.	Betydande påverk-an på -förtroende från medarbetare eller allmänheten.	Allvarlig och långvarig påverkan på förtroende från medarbetare eller allmänheten.

Tabell 7. Linköpings kommuns konsekvenstabell.

Bilden visar två händer som antecknar i ett anteckningsblock.

Informationsruta

Så här används konsekvenstabellen
Informationsklassningen utförs med hjälp av konsekvenstabellen genom att skadan för respektive informationssäkerhetsaspekt identifierar vilket konsekvensområde som är aktuellt för den informationstyp/handling som bedöms.

Det är alltid den värsta tänkbara, mest allvarliga och omfattande konsekvensen som ska styra och anges som resultat för respektive informationssäkerhetsaspekt, oavsett konsekvensområde. Om konsekvensen för att en informationstyp/handling är otillgänglig t.ex. medför tre tydliga konsekvenser enligt följande:

- Kommunen får betala 1 miljon i sanktionsavgift pga. icke uppfyllda krav -> allvarliga (3) ekonomiska konsekvenser.
- Kommunens arbete försenas allvarligt -> betydande (2) verksamhetskonsekvenser.
- Kritik i media under kort tid - > måttliga (1) konsekvenser på verksamhetens anseende.

Den högsta konsekvensnivån för tillgänglighet är den ekonomiska, dvs. allvarlig konsekvens (3). Skyddsbehovet avseende tillgänglighet för informationstypen/handlingen är därmed skyddsnivå 3.

Motsvarande princip gäller för informationssäkerhetsaspekterna, Riktighet, Tillgänglighet och Spårbarhet dvs. vilka konsekvenser som uppträder om informationstypen/handlingen inte är riktig, inte är tillgänglig respektive inte går att spåra.

Bedömning av konfidentialitet utgår bara från de konsekvenser ett röjande medför i förhållande till lagstiftning.

Juridiska konsekvenser bedöms främst utifrån verksamheten

En juridisk konsekvens för kommunen kan delas in i två områden. Det som avser kommunen som verksamhet och det som avser den enskilda medarbetaren. Konsekvenserna och deras följder är inte likadana. Kommunen kan bryta mot lag med följder som exempelvis sanktioner eller allvarlig kritik från myndighet, men en kommun kan aldrig dömas till fängelse.

Konsekvenstabellen utgår inte från juridiska konsekvensen för medarbetare utan enbart sådana som berör kommunen som verksamhet.

Påverkan inom ett konsekvensområde resulterar ofta i en sekundär konsekvens inom ett annat område. Exempelvis kan negativ påverkan för en individ leda till att kommunens anseende påverkas, och påverkan på verksamhetens förmåga kan medföra juridiska konsekvenser. Ta därför alltid hänsyn till sådana samband när konsekvenstabellen används för att identifiera värsta tänkbara konsekvens för kommunen. I klassningen anges endast ett värde per infor-mationssäkerhetsaspekt. Detta värde ska överensstämma med värsta tänkbara konsekvens, vilket då uttrycker informationstypens skyddsbehov på ett korrekt sätt.

3.7.5 Klassningens resultat

Klassning utförs för varje handlingstyp i IHP:n och analyserar konsekvenser för samtliga fyra informationssäkerhetsaspekter. Konsekvensnivån ska motsvara de skyddsåtgärder som krävs för att skydda informationen så verksamheten inte skadas.

Utifrån samtliga fyra aspekter får informationstypen/handlingen ett skyddsbehov. Nedan följer ett antal fiktiva exempel på skyddsbehov för olika informationstyper/handlingar.

Informationstyp/handling	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
Skolmatsalsmeny (rätter)	0	3	1	1
Skolmat (ingredienser)	0	3	1	2
Elevakt	2	2	1	2
Öppettider badhus	0	1	1	0
Personalakt	2	2	1	2
Familjeutredning	3	2	2	2
Leverantörsanbud	2	3	1	2
Krisplan	3	3	3	2

Tabell 8. Exempel på olika skyddsbehov.

Informationsruta

Ovanligt med låga konsekvenser för vissa aspekter
Det är ytterst ovanligt att informationssäkerhetsaspekterna riktighet, tillgänglighet och spårbarhet bedöms med ingen eller lindrig konsekvens och hamnar på skyddsnivå 0. Orsaken till detta är att vi oftast förutsätter att information ska vara riktig, tillgänglig och spårbar; om den inte är det så kan det vara svårt att över huvud taget använda informationen. Därför kräver de flesta informationstyper ett grundskydd utifrån dessa tre aspekter och klassas vanligen minst till skyddsnivå 1.

Handlingen Krisplan ger utifrån informationsklassningen skyddsbehovet 3–3–3–2. I exemplet krisplan betyder detta att ett högt skydd krävs inom tre informationssäkerhetsaspekter och förhöjt skydd inom en informationssäkerhetsaspekt. Vilka faktiska skydd som krävs och vem som ansvarar för detta beslut kommer att visas senare i handboken.

Nedan följer ett antal fiktiva exempel på skyddsåtgärder kopplat till skydds-nivå och informationssäkerhetsaspekt, vilka redovisar principer där skydds-behovet ökar. Kapitel 2, 5 och 6 innehåller specifika skyddsåtgärder för hanteringsregler, it-säkerhet och fysiska skydd.

Informationssäkerhetsaspekt				
Skyddsnivå	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**	**Spårbarhet**
3. Röd: Högt skyddsbehov	Kryptering och tvåfaktorsautentisering.	Dubblerad kontroll av ny och förändrad information.	Redundanta system	Loggning av samtliga användarhändelser.
2. Orange: Förhöjt skyddsbehov	Inloggning med tvåfaktorsautentisering.	Dubblerad kontroll av ny information.	Spegling av databas.	Loggning av förändringar i system.
1. Gul: Grundläggande skyddsbehov	Inloggning med personliga konton och lösenord.	Kontroll av ny och förändrad information.	Regelbunden säkerhetskopiering.	Loggning av inloggningar.
0. Grön: Inget skyddsbehov	Ingen inloggning krävs.	Ingen kontroll av ny eller förändrad information krävs.	Ingen säkerhetskopiering krävs.	Ingen loggning krävs.

Tabell 9. Exempel på skyddsåtgärder för it-säkerhet för olika skyddsnivåer.

I det tidigare exemplet (tabell 6) fick handlingen Personalakt skyddsbehovet 2–2–1–2. Med hjälp av tabell 7 utläser vi då att inloggning till personalakten måste ske med tvåfaktorautentisering, att två personer ska godkänna en ny akt, att det ska finnas regelbunden säkerhetskopiering och att det sker loggning av användare som ansluter sig till det it-system där personalakten lagras.

3.7.6 Användningsområden och målgrupper för klassningen

Klassningsmodellen vänder sig dels till informationsägare, dels till dem som på något sätt ansvarar för att rätt skydd implementeras och upprätthålls. Den klassade informationen utgör ett underlag för verksamheter vid kravställning av tjänster, exempelvis it-tjänster och it-system, både internt och externt. Modellen fungerar på så sätt som en

kommunikationsmodell med medarbetare samt mellan beställare och leverantör av tjänster och system.

Information bör identifieras och klassas initialt när informationssäkerhetsbehovet ska analyseras men även löpande och när verksamheter eller it-system förändras.

3.7.7 Informationsklassernas relation till lagar och föreskrifter

Kommunens informationsklasser inom konfidentialitet är helt kopplade till det juridiska konsekvensområdet. Inom Riktighet, Tillgänglighet och Spårbarhet bedöms konsekvenser inom både juridik och andra konsekvensområden.

En begäran om utlämnande av allmän handling ska alltid ske enligt offentlighets- och sekretesslagen, oavsett vilken informationsklass den aktuella informationen tillhör. Det innebär att information som klassats som stark sekretess efter en sekretessprövning ändå kan komma att lämnas ut med stöd av offentlighetsprincipen.

3.7.8 Olika perspektiv på riktighet, tillgänglighet och spårbarhet

Informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet är ursprungligen härledda från engelskans CIA-begrepp (confidentiality, integrity och availibility). Översättningen från det engelska ordet integrity till svenskans

riktighet är egentligen lite missvisande eftersom det som egentligen avses är informationens riktighet ur perspektivet korrekthet eller autenticitet. Även giltighet och aktualitet ur perspektivet om information är härledd eller inhämtad kan avses med riktighet. Ur dessa perspektiv kan man se riktigheten även som ett mått på informationens kvalitet.

Översättningen av availibility till tillgänglighet är tydligare men säkerhetsaspekten tillgänglighet kan även ses utifrån två perspektiv:

- Tillgänglighet (korttid), dvs. hur länge verksamheten klarar sig utan informationen. Vanligen uttrycks detta behov i timmar, dygn eller någon vecka.
- Tillgänglighet (långtid), dvs. hur länge informationen bevaras. Vanligen uttrycks detta behov i månader, år eller kanske t.o.m. årtionden.

Dessa två perspektiv kan användas för att komplettera konsekvenstabeller när det finns krav på att differentiera aspekten tillgänglighet. Dessa två perspektiv på tillgänglighet kallas även tillgänglighet I (korttid) respektive tillgänglighet II (långtid).

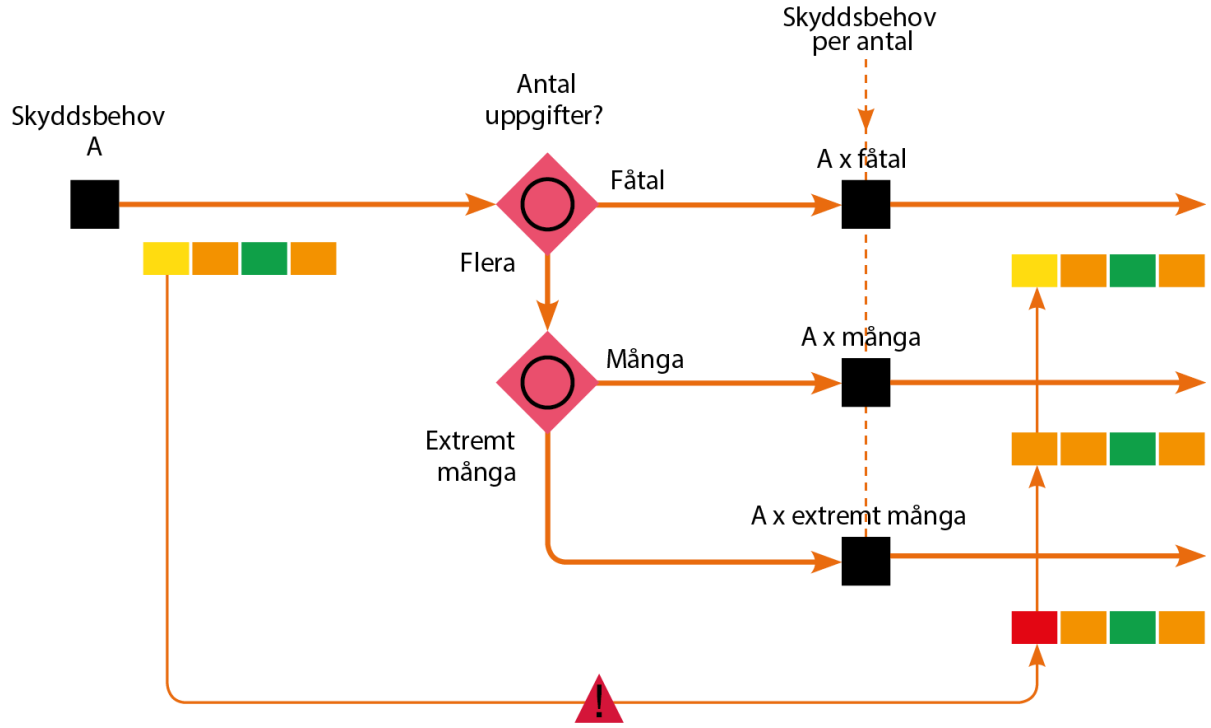
Även informationssäkerhetsaspekten spårbarhet kan ses utifrån två perspektiv:

- Direkt spårbarhet, dvs. behovet av att veta vem som har gjort vad och när.
- Återställbarhet, dvs. behovet att kunna återskapa information till sitt ursprung vid en given tidpunkt bakåt i tiden.

Även återställbarhet bör användas i konsekvenstabeller om omständigheterna kräver det. Dessa två perspektiv kallas även spårbarhet I (direkt spårbarhet) och spårbarhet II (återställbarhet).

3.7.9 Antalet uppgifter kan styra klassning

Vid informationsklassning kan mängden uppgifter ibland avgöra hur omfattande en konsekvens blir för verksamheten. Ta personuppgifter som exempel: Om en enskild personuppgift röjs kanske konsekvensen är liten men om en databas med tusentals personuppgifter röjs blir sannolikt konsekvensen betydligt mer omfattande och kan leda till en högre klassning.



Figur 23. Antalet uppgifter kan skapa behov av en högre bedömning. Figuren visar en processkarta över antalet uppgifter från ett skyddsbehov. Uppgifterna delas in i 4 kategorier: ett fåtal, flera, många och extremt. De olika uppgifterna får x-antal skyddsbehov beroende på vilken kategori de tillhör.

Motsvarande resonemang kan tillämpas på fler områden där mängden uppgifter är relevant. En konsekvenstabell bör därför kompletteras med ett perspektiv på antal uppgifter om omständigheterna vid klassningen kräver detta.

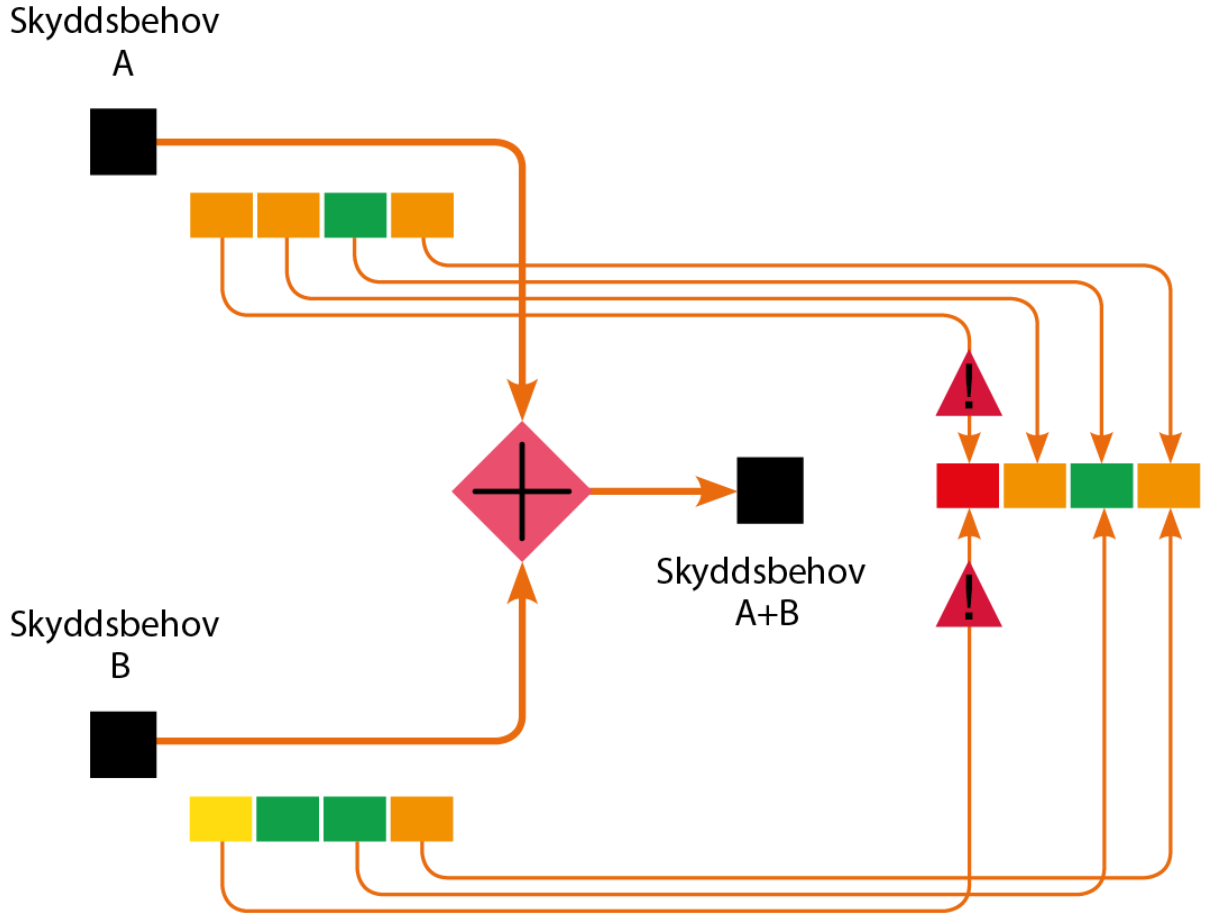
Informationsruta
Fler uppgifter betyder inte med säkerhet högre klass

Om informationsägaren redan klassat ett litet antal uppgifter med högsta skyddsbehovet så blir inte klassningen ännu högre bara för att antalet uppgifter ökar. Däremot kan ett sådant förhållande indikera att kompletterande riskanalyser kan vara nödvändiga.

3.7.10 Kombinerad information kan ändra klassning

I vissa situationer kan klassningen ändras när enskilda informationstyper kombineras med varandra. Detta gäller inte minst personuppgifter.

Exempelvis kan handlingar klassas med sekretess på grund av att de innehåller känsliga personuppgifter. Om man hanterar en sådana handlingar tillsammans med annan information om t.ex vårdkontakter, omdömen eller relationer så kan de istället klassas som stark sekretess eftersom det dels är en större mängd känsliga personuppgifter dels ger en mer detaljerad bild av en enskild person.



Figur 24. Kombinerad information skapar ny informationsklassning. Figuren visar två olika skyddsbehov (A och B) i form utav två rutor som sedan kombineras till ett enda skyddsbehov (A+B). UNder varje skyddsbehov finns olika informationstyper i olika klassningar. Klassningarna dessa visas med hjälp av i färgerna: gul, grön och orange. Klassningen ändras när de enskilda informationstyper kombineras med varandra. Figuren visar att två orangea i kombination, blir röd och får en varningstriangel.

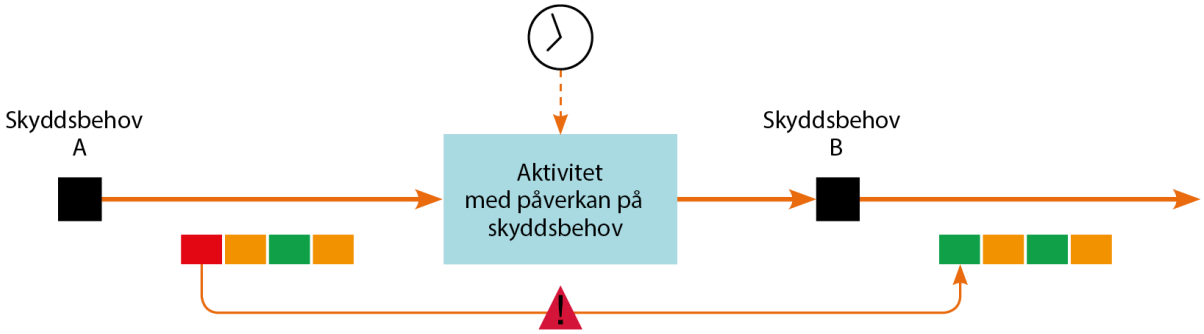
Kombinationen kanske inte kan bli högre

Här gäller samma förhållande som på föregående sida – att den kombinerade informationstypen kan inte tilldelas en högre klass om de ingående typerna redan har den

högsta klassen. Däremot kan den begränsade grupperingen av typerna skiljas åt. Även här kan ett sådant förhållande indikera att kompletterande riskanalyser är nödvändiga.

3.7.11 Tiden kan påverka klassning

Även tid är en faktor som kan påverka klassningen av en informationstyp. Det är vanligt att viss information ändrar informationsklass över tid. Ett vanligt exempel är informationstypen upphandlingsunderlag. Denna informationstyp har ofta en hög nivå av konfidentialitet fram till den dag när underlaget blir en anbudsförfrågan och presenteras samt görs offentlig. Efter presentationen förändras klassningen av konfidentialitet från relativt hög nivå till den lägsta nivån (öppen information). Motsvarande situationer kan även finnas för de andra informationssäkerhetsaspekterna, exempelvis höga krav på tillgänglighet i närtid i en specifik situation, där kraven sänks när informationstypens aktualitet minskar.



Figur 25. Visar en processkarta där tid kan påverka klassning hos en informationstyp. Processkartan visar en ruta med skyddsbehov A med en pil som går igenom en ruta med en klocka och titeln “Aktivitet med på verkan av skyddsbehov”. Pilen fortsätter sedan vidare mot skyddsbehov B, en svart ruta på andra sidan.

Tidens påverkan i kommuner

Hos en kommun är en av de vanligaste orsakerna till att en klassning ändras att sekretessen för en handling upphör efter en viss tid.

Om faktorn tid påverkar en viss informationstyp är det vanligt att dela upp -informationstypen i flera informationstyper, t.ex. upphandlingsunderlag -respektive anbudsförfrågan. När upphandlingsunderlaget förbereds används en informationstyp och när det har presenterats byter man informationstyp.

Det ska framgå av konsekvenstabellerna att en verksamhet hanterar informations-typer där tiden är en faktor.

ID	Regler och anvisningar för informationsklassning
S 7.1	En gemensam modell för informationsklassning ska finnas och

0 1 2 3	gälla samtliga verksamheter inom Linköpings kommun.
S 7.2 0 1 2 3	Linköpings kommuns modell för informationsklassning ska tillämpas vid kravställning på informationssäkerhet. Genom att information klassas enligt modellen kan behov av skyddsåtgärder kopplas till de olika nivåerna i klassningsmodellen.

3.8 Risker och hantering av risker

En riskanalys innebär att man identifierar de hot och brister som är riktade mot en verksamhet, en tjänst eller ett system samt värderar sannolikheten för att de förverkligas och konsekvenserna om de förverkligas. Det är framför allt -informationsägare, informationsresursägare och projektbeställare som kan behöva göra riskanalyser gällande informationssäkerhet för att minska sannolik-heten för och konsekvenserna av hot och brister. Riskanalyser kan även ske på informationssäkerhetssamordnarens initiativ för att upptäcka risker på väsentliga- delar inom kommunen.

En riskanalys omfattar följande steg:

- Identifiering av risker: Vilka risker utsätts vi för?
- Värdering av risker: Vilken är sannolikheten och vilka blir konsekvenserna?
- Hantering av risker: Ska vi åtgärda eller acceptera?

(Metoden för att genomföra riskanalyser beskrivs i detalj i kapitel 4.8 – Analys och hantering av risker.)

Ansvar för riskanalyser		Fördjupad information
●	Alla medarbetare med en utpekad informationssäkerhetsroll har ett uttalat ansvar för att initiera riskanalyser när man befarar att aktuell skyddsnivå inte når upp till behovet av skydd. Det finns dock inget hinder för andra roller att initiera riskanalyser.	Kapitel 4.8 – Analys och hantering av risker

Riskanalyser med fokus på informationssäkerhet ska alltid genomföras när det existerar ett gap mellan behov av skyddsnivå och det faktiska skyddet (i nuläget), (se kapitel 3.6 – Informationsklassningens grunder). Andra situationer som kan aktivera behovet av en riskanalys är vid

- förändrad verksamhet, t.ex. omorganisation, flytt, större förändrad användning eller ändrad hantering av informationstyper
- start av projekt där värdefull information kan komma att hanteras
- behov av ett underlag för kontinuitetsplaner
- förändrad användning av it-system
- upphandling av nya it-system
- större förändringar gällande vilka medarbetare som har tillgång till en viss informationstyp
- utredning gällande avsteg från krav under informationsklassning
- andra situationer när det kan förväntas att riskerna förändras.

En riskanalys riktad mot informationssäkerhet förutsätter att

- en riskägare utses för varje risk där riskägaren har behörighet att avgöra riskbehandling eller riskacceptans utifrån givna kriterier
- konsekvensskalan används för att bedöma konsekvenser och säkerställa en jämförbar bedömning mellan riskanalyser
- en ansvarig för genomförande utses vid beslut om riskbehandling; denna person ska acceptera uppdraget och godkänna tidsplaneringen
- en riskanalys är komplett och avslutad när alla beslutade åtgärder är genomförda eller på annat sätt stängda.

Resultaten från riskanalyser ska bevaras i skriftlig form, inklusive resultaten från beslut om åtgärder och accepterade risker. Resultaten ska även delges informationssäkerhetssamordnaren, som ansvarar för kommunens samlade riskbild. Resultaten kan även bli föremål för uppföljning för att säkerställa att processen för riskhantering efterlevs. Riskanalysrapporten är en egen informationstyp. Den innehåller ofta skyddsvärd information och ska i så fall klassas som sekretess eller stark sekretess.

ID	Regler och anvisningar för hantering av risker
S 8.1 0 1 2 3	Riskanalyser med fokus på informationssäkerhet ska genomföras när det existerar ett gap mellan skyddsbehov och faktiskt skydd. Även misstanke om att gap kan utgöra grund för en riskanalys.
S8.2 0 1 2 3	Resultat från riskanalyser ska dokumenteras och delges informationssäkerhetssamordnaren.
S 8.3 0 1 2 3	En riskägare ska utses för varje risk. Riskägaren har behörighet att avgöra riskbehandling eller riskacceptans.

3.9 Skyddsåtgärder

Krav på skyddsåtgärder styrs av informationsklassning. Inom varje skyddsområde, arbetssätt, it-teknik och fysiska skydd, finns detaljerade krav föreskrivna för varje informationsklass, se figur 21.

Om de krav på skydd som faller ut från Informationsklassning bedöms vara svåra att realisera eller inte ge tillräckligt skydd så genomförs en riskanalys -(se stycke 3.8 och regel S8.1).

Avsteg från föreskrivna skyddsåtgärder betraktas som risker och som sådana kan de antingen bemötas med andra skyddsåtgärder eller accepteras av riskägare. Beslutsprocess för acceptans av risker beskrivs i stycke 3.6 och 3.13. Som grund-princip bör både Informationsägare och resursägare vara överens om den föreslagna lösningen eller acceptans av risk.

Se även Kapitel 4, styckena 4.8.4 och 4.8.5

3.10 Personalsäkerhet

Medarbetaren är den viktigaste resursen i kommunen och många medarbetare hanterar dagligen information manuellt eller med stöd av it. Många kommer också i kontakt med och hanterar viktig information. Därför är det av största vikt att alla medarbetare får information och utbildning om informationssäkerhet. Det är också viktigt att det finns rutiner i verksamheten när någon anställs, byter arbetsuppgifter eller avslutar sin anställning.

Ansvar för personalsäkerhet	Fördjupad information

●	Rekryterande chef ansvarar för att regler och anvisningar gällande informationssäkerhet efterföljs.	Kapitel 4.3 – Chefer och verksamhetsansvariga
●	För befattningar som har betydelse för Sveriges säkerhet ansvarar säkerhetsskyddschefen för att säkerhetsprövning sker.	Kapitel 4.3 – Chefer och verksamhetsansvariga Kapitel 7.2.4 – Lagar och regelverk som relaterar till informationssäkerhet

3.10.1 Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Linköpings kommun sker genom att den sökandes meritförteckning verifieras, t.ex. genom kontakt med referenser samt kontroll av uppgivna akademiska och yrkesmässiga kvalifikationer. Identitetskontroll av sökande ska även utföras före en anställning.

Nyanställda ska

- få information om ansvar och skyldigheter kopplade till informationssäkerhet
- få utbildning i informationssäkerhet
- ta del av informationssäkerhet för medarbetare enligt denna handbok.

För vissa kritiska tjänster krävs en förstärkt kontroll, vilken kan innefatta kreditupplysning eller kontroll i brottsregister. Exempelvis på kritiska tjänster är vissachefstjänster eller tjänster där den anställda har åtkomst till information med stark sekretess. Självklart följer kommunen lagstiftningen avseende registerkontroll för skydd av barn och unga.

För befattningar som har betydelse för Sveriges säkerhet ombesörjer säkerhetsskyddschefen att en säkerhetsprövning med registerkontroll sker. Placering i säkerhetsskyddsklass är ett krav för att få arbeta med verksamhet som har betydelse för Sveriges säkerhet. De befattningar som är aktuella i detta sammanhang framgår av Linköpings kommuns säkerhetsskyddsplan.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning om personuppgifter.

Information och utbildningar ska ges kopplat till det ansvar som följer med en viss roll, t.ex. informationsägarskap. Alla anställda som har tillgång till information med stark sekretess ska underteckna blankett för tystnadsplikt, vilken gäller även efter att anställningen upphört. Detta avtal inskränker dock inte medarbetares lagliga rätt till yttrandefrihet och meddelarfrihet.

ID	Regler och anvisningar för personalsäkerhet före och i samband med anställning
S 10.1 0 1 2 3	Identitets- och bakgrundskontroll av sökande ska göras före anställning, där den sökandes meritförteckning verifieras.
S 10.2 0 1 2 3	Vid anställning till kritiska tjänster ska sökande genomgå en förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister.
S 10.3 4	Placering i säkerhetsskyddsklass är ett krav för att få arbeta med verksamhet som har betydelse för Sveriges säkerhet.
S 10.4 0 1 2 3	Nyanställda ska informeras om ansvar och skyldigheter kopplade till informationssäkerhet, utbildas i informationssäkerhet samt ta del av denna handbok och annat ansvar som följer med respektive roll, t.ex. vid informationsägarskap.
S 10.5 3	Samtliga medarbetare som hanterar information med stark sekretess ska underteckna blankett för tystnadsplikt.

3.10.2 Under anställning

Kommunens medarbetare ska vara medvetna om och följa gällande regler och anvisningar för informationssäkerhet.

Alla medarbetare, och externa deltagare i förekommande fall, ska få utbildning så att de kan följa reglerna och anvisningarna i denna handbok.

Roller med särskilt ansvar inom informationssäkerhet, t.ex. informationsägare, objektägare, it-säkerhetsamordnare, ska få relevant fortbildning inom området.

ID	Regler och anvisningar för personalsäkerhet under anställning

S 10.6 0 1 2 3	Alla medarbetare, och externa aktörer i förekommande fall, ska få lämplig utbildning för att kunna följa kommunens handbok för informationssäkerhet.
S 10.7 0 1 2 3	Roller med särskilda uppgifter inom informationssäkerhet ska få relevant fortbildning inom området.

3.10.3 Vid upphörande eller ändring av anställning

Tystnadsplikt gäller även efter att en anställning förändrats eller upphört. Ansvar och skyldigheter för informationssäkerhet definieras och kommuniceras vid anställningstillfället.

I direkt samband med avslut eller ändring av anställning ska it-resurser återlämnas och åtkomsträttigheter till information och it-resurser dras in.

ID	Regler och anvisningar för upphörande eller ändring av anställning
S 10.8 0 1 2 3	Alla medarbetare, och externa aktörer i förekommande fall, ska få lämplig utbildning för att kunna följa kommunens handbok för informationssäkerhet.
S 10.9 0 1 2 3	Roller med särskilda uppgifter inom informationssäkerhet ska få relevant fortbildning inom området.

3.11 Leverantörsrelationer

Det är många faktorer att ta hänsyn till när kraven i ett underlag inför upphandling ska formuleras. Att säkerställa skyddet av den information som den externa parten, dvs. leverantören, ska hantera är en sådan faktor.

Ansvar vid leverantörsrelationer		Fördjupad information
●	Den som initierat en upphandling ansvarar för att relevanta informationssäkerhetskrav inkluderas.	Kapitel 5.10 – Informations-säkerhetskrav vid upphandling

Reglerna och anvisningarna i denna handbok ska användas som informationssäkerhetskrav vid extern upphandling av verksamhetsstödjande tjänster, t.ex. it-tjänster, vårdtjänster och lokalvårdstjänster.

ID	Regler och anvisningar gällande leverantörsrelationer
S 11.1	Behovet av säkerhet vid en upphandling ska baseras på regler

	och anvisningar i denna handbok kopplat till kommunens modell för informationsklassning.

3.12 Efterlevnad och granskning

Efterlevnaden av dokumenten Säkerhetspolicy, Riktlinjer för informationssäkerhet och Handbok för informationssäkerhet ska följas upp. I praktiken innebär det främst att

- kraven i handboken granskas och följs upp
- regler och anvisningar efterlevs
- säkerhetsåtgärder införs och får avsedd verkan.

Ansvar vid leverantörsrelationer		Fördjupad information
●	Informationssäkerhetssamordnaren tillsammans med informationssäkerhetsrådet ansvarar för -uppföljning av efterlevnad och att granskning sker av kommunens informationssäkerhet.	Kapitel 3.4.1 – Informations-säkerhetssamordnaren Kapitel 3.4.3 – Informations-säkerhetsrådet Kapitel 3.3.5 – Informationsägare

I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och it-resurser med förhöjda och höga skyddsbehov.

Informationssäkerheten och dess styrning ska granskas och följas upp kontinuerligt samt hanteras i verksamhetens planering. Det är Informations-ägarens ansvar att det sker.

Uppföljning av Linköping kommuns informationssäkerhet ska göras minst vart fjärde år. Uppföljningen av informationssäkerhet ska även inkluderas i kommunens internkontrollplan.

Sårbarheter och brister som upptäcks vid olika granskningar tas upp för åtgärd i olika genomförandeplaner, t.ex. objektplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Större sårbarheter och brister ska rapporteras som risker till informationssäkerhetssamordnaren.

Granskning av säkerheten för it-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att en tillräcklig skyddsnivå upprätthålls. (Se vidare i kapitel 5 – Informationssäkerhet i it-nära förvaltning.)

ID	Regler och anvisningar för efterlevnad och granskning av informationssäkerhet
S 12.1 0 1 2 3	Efterlevnaden av Säkerhetspolicy, Riktlinjer för informationssäkerhet och Informationssäkerhetshandboken ska följas upp. Informationssäkerhetsrådet ansvarar för att så sker.
S 12.2 0 1 2 3	Efterlevnaden ska ske genom uppföljningar och även vara inkluderad i kommunens internkontrollplan.

3.13 Dispenser och undantag från handboken

Handbokens regler och anvisningar gäller all hantering av information och ska alltid tillämpas. I undantagsfall kan det finnas situationer där handbokens regler och anvisningar inte behöver följas. Alla sådana situationer kräver dock att en ansökan om dispens ställs till kommunens informationssäkerhetsråd.

Ansvar för dispenser och undantag		Fördjupad information
●	Kommundirektören ansvarar för att godkänna eller neka dispenser och undantag från informationssäkerhetshandboken s regler och anvisningar.	Kapitel 3.3 – Organisation och ansvarsfördelning

ID	Regler och anvisningar för dispenser och undantag
S 13.1 	Dispenser och undantag ska alltid behandlas i informations-säkerhetsrådet och beslutas av kommundirektören.

Kapitel 4 - Informationssäkerhet i verksamhetsnära förvaltning

4.1 Inledning

Detta kapitel vänder sig till samtliga chefer i Linköpings kommun och till dem som har roller inom pm3, eftersom dessa personer utgör en viktig del av arbetet med informationssäkerhet. Kapitel 4 behandlar också hur informationssäkerhetsroller interagerar i det verksamhetsnära förvaltningsarbetet. Därför beskrivs centrala processer som t.ex. informationsklassning och riskanalys mer ingående utifrån verksamhetsnära kontext.

4.2 Verksamhetsnära roller och ansvar

I kapitlet finns regler och anvisningar som gäller dels för chefer och verksamhetsansvariga, dels för olika roller inom pm3 och den verksamhetsnära förvaltningen. I kapitel 5, som riktar sig till den som arbetar i kommunens it-verksamhet, återfinns regler och anvisningar som gäller informationssäkerhet i den it-nära förvaltningen, och i kapitel 6 återfinns regler och anvisningar som gäller fysiskt skydd.

4.3 Chefer och verksamhetsansvariga

I varje chefsbefattning ingår ansvar för att med-arbetare får tillräcklig utbildning om informations-säkerhet, bl.a. om regler och anvisningar i denna handbok. En chef har också ansvar för att handbokens regler och anvisningar är kända av medarbetarna och för att säkerställa stöd till med-arbetarna i frågor som rör informationssäkerhet. -Chefens ansvar för informationssäkerhet kan aldrig -överlåtas; däremot kan relaterade arbetsuppgifter överlåtas.

Varje chef ska se till att alla medarbetare som hen ansvarar för vet hur		Fördjupad information
●	det egna ansvaret för informationssäkerhet ser ut, dvs. att lagar och regler följs och att medarbetarna har en skyldighet att rapportera incidenter och brister	Kapitel 2.2 – Samtliga medarbetare ansvarar för informationssäkerheten
●	olika typer av information ska hanteras och hur informationen får förmedlas	Kapitel 2.3 – Informationsklasser för konfidentialitet (konfidentialitetsklasser) Kapitel 2.4 – Säkert beteende Kapitel 2.8 – Digital kommunikation (e-post, chatt, distansmöten)
●	säkra lösenord skapas och skyddas samt vad man gör om lösenordet röjs till obehöriga	Kapitel 2.5 – Identifiering, inloggningskonton och behörigheter
●	mobila enheter (bärbar dator, smarttelefon, surfplatta) hanteras och hur arbete på distans utförs	Kapitel 2.6 – Mobila enheter och arbete på distans
●	hen skyddar sig mot skadlig kod	Kapitel 2.7 – Skadlig kod
●	internet ska användas och vad varje medarbetare ska tänka på vid användning av sociala medier	Kapitel 2.9 – Internet och sociala medier
●	information ska lagras	Kapitel 2.10 – Lagring och säkerhetskopiering
●	användning av molntjänster får ske	Kapitel 2.11 – Molntjänster
●	spårbarhet hanteras och vad som gäller för loggning	Kapitel 2.12 – Spårbarhet och loggning
●	eventuella kompletterande regler för informationssäkerhet i den egna verksamheten följs	Kapitel 3.3.3 – Ansvar inom respektive verksamhet

Varje chef har också ansvar för att det fysiska skyddet överensstämmer med den information som hanteras i verksamheten (se vidare kapitel 6 – Informationssäkerhet och

fysiskt skydd). I det fall en chef varken har mandat eller medel att se till att det fysiska skyddet är i paritet med handbokens krav på skydd registreras detta som en risk och informationssäkerhetssamordnaren informeras. Om du som chef inte har mandat att agera, sök vägledning hos informationssäkerhetssamordnaren.

ID	Regler och anvisningar för efterlevnad och granskning av informationssäkerhet
V 3.1 0 1 2 3	Medarbetare ska få relevant och tillräcklig utbildning i dels informationssäkerhet så att regler och anvisningar i denna handbok följs, dels eventuella informationssäkerhetsregler som gäller den egna verksamheten.
V 3.2 0 1 2 3	Skyddsåtgärder för det fysiska skyddet ska vara implementerade i förhållande till den informationsklass som hanteras i verksamheten.

Chefer och verksamhetsansvariga har ett ansvar för att agera förebyggande och se till att informationssäkerheten inte äventyras. Vid större förändringar (se exempel nedan) ska verksamheten analysera om det finns risker som påverkar informationssäkerheten (se även kapitel 4.8 – Analys och hantering av risker).

Resultatet från en riskanalys redovisas till informationssäkerhetssamordnaren, och hen har sedan ansvar för att sammanställa en total bild över kommunens informationssäkerhetsrisker. Det kan vara lämpligt att analysera risker när

- ett nytt projekt påbörjas där verksamheten kan komma att hantera information som klassats i högre skyddsnivåer
- ny typ av information ska produceras; här gäller även informationsklassning
- det kommer nya lagkrav eller ny praxis där hänsyn behöver tas till hantering av viss information
- någon slutar som har tillgång till information som klassats med höga skyddsnivåer, framför allt om personen skilts från sin tjänst på ofrivillig grund.

ID	Regler och anvisningar för chefer och verksamhetsansvariga
V 3.1 0 1 2 3	Vid förändringar som kan ha större påverkan på verksamhetens informationssäkerhet ska en riskanalys genomföras och redovisas till informationssäkerhetssamordnaren.

4.5 Informationssäkerhet för roller i den verksamhetsnära förvaltningen

För mer information gällande pm3 och hur modellen fungerar för it-styrning i kommunen, se Linweb.

4.5.1 Objektstyrgrupp

I objektstyrgruppen ingår representanter för den verksamhetsnära förvaltningen och för it. Gruppen ansvarar gemensamt för objektets it-utveckling, förvaltning och informationssäkerhet, där det bl.a. ingår att följa reglerna i denna handbok.

Om inte fastställd skyddsnivå nås i förvaltningsobjektet är det objektstyrgruppens ansvar att antingen tillsätta resurser för åtgärd eller ange skälet till att man väljer en annan skyddsnivå. I vissa fall ska och kan ett sådant beslut enbart tas av nämnd. I bägge fallen ska beslutet dokumenteras som en risk och redovisas till informationssäkerhetsrådet och till informationsägaren.

Ansvar för objektstyrgrupp		Fördjupad information
●	Gruppen ansvarar gemensamt för objektets informationssäkerhet. Om fastställd skyddsnivå inte nås för objektet ansvarar objektstyrgruppen för att tillsätta resurser eller ange skäl till avsteg, alternativt vidarebefordra beslut till nämnd.	Kapitel 4.7.5 – Vikten av att tilldela lämpliga informationsklasser

4.5.2 Objektägare verksamhet

Objektägare verksamhet är ansvarig för att sammanställa informationsägarens informationsklassning och omvandla den till skyddsbehov. Behovet ger svar på vilka skyddsåtgärder som ska implementeras för respektive it-komponent. Om en it-komponent hanterar flera typer av information är det typen med högst klassning som styrskyddsbehovet. Med andra ord styr informationen som hanteras i en it-komponent vilka skyddsåtgärder som behövs.

Ansvar som objektägare verksamhet		Fördjupad information
●	Gruppen ansvarar gemensamt för objektet informationssäkerhet. Om fastställd skyddsnivå inte nås för objektet ansvarar objektstyrgruppen för att tillsätta resurser eller ange skäl till avsteg, alternativt vidarebefordra beslut till nämnd.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.2 – It-nära roller och ansvar Kapitel 6.2 – Allmänt om säkerhet och fysiskt skydd

4.5.3 Objektledare verksamhet

Objektledare verksamhet leder förvaltningsarbetet. I ansvaret ingår att se till it-komponenterna får fastställd skyddsnivå och att alla relevanta informationssäkerhetsåtgärder genomförs. Objektledaren ska också rapportera till objektägare verksamhet om någon it-komponent inte når fastställd skyddsnivå. Objektledarens motsvarighet i den it-nära förvaltningen är objektledare it. Objektledaren kan vid behov överlåta arbetsuppgifter till objektspecialister.

Ansvar som objektledare verksamhet		Fördjupad information
●	Objektledare verksamhet ansvarar för att it-komponenter får fastställd skyddsnivå.	Kapitel 5.3 – Hantering av tillgångar
●	Objektledare verksamhet ansvarar för att rapportera till objektägare verksamhet om någon it-komponent inte når upp till fastställd skyddsnivå.	Kapitel 5.3 – Hantering av tillgångar

4.5.4 Objektspecialist

Objektspecialisten ansvarar för att utföra aktiviteter relaterade till informationssäkerhet på uppdrag av objektledaren. Motsvarigheten i den it-nära förvaltningen kallas it-specialist.

Ansvar för objektspecialist		Fördjupad information
●	Objektspecialisten ansvarar för att utföra aktiviteter relaterade till informationssäkerhet på uppdrag av objektledaren.	Kapitel 5.3 – Hantering av tillgångar

4.5.5 Objektägare it och objektledare it

Dessa roller är knutna till den it-nära förvaltningen och redovisas i kapitel 5. (se kapitel 5.2 – It-nära roller och ansvar).

4.5.6 Kommunikation mellan informationsägare och objektägare verksamhet

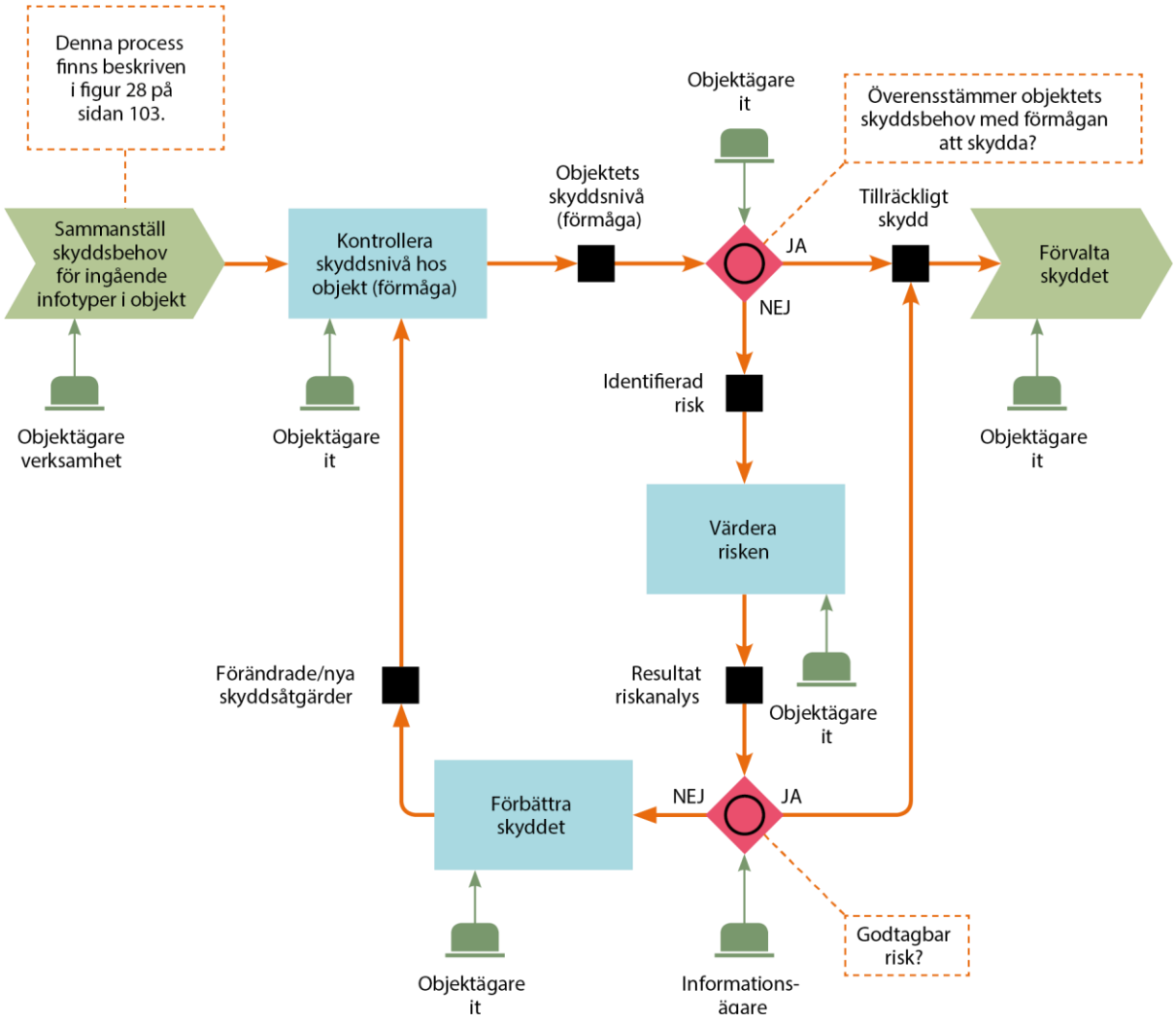
En informationsägare (vanligen förvaltningschef) ansvarar för att informationsklassningen genomförs och beslutar också om informationens slutgiltiga klassning (se även kapitel 3.4 – Informationssäkerhetsorganisation och kapitel 4.7 – Informationsklassning).

Klassningen ger underlag för att beskriva informationens skyddsbehov. Informationsägaren ansvarar för att förmedla underlaget till den eller de objektägare verksamhet som ansvarar för det objekt som hanterar informationen.

Objektägare verksamhet ansvarar för att sammanställa samtliga informationsägares klassningar till ett skyddsbehov för objektet/objekten. Praktiskt kommer objektägare verksamhet överföra behovet av it-tekniska skyddsåtgärder till it-nära förvaltning och objektägare it. Objektägare it återrapporterar sedan till objektägare verksamhet huruvida man kan tillgodose önskad skyddsnivå. Säkerhetsåtgärder som ingår i skyddsnivån men

som inte har realiserats ska redovisas som kvarstående risker till objektägare verksamhet, som sedan redovisar riskerna till informationsägarna.

Om det finns ett gap mellan skyddsbehovet och förmågan att skydda information i ett objekt ansvarar objektägare verksamhet tillsammans med objektägare it för att hantera dessa risker.



Figur 26. Informationsägare kopplat till objektägare verksamhet och objektägare it. Figuren visar en processkarta över informationsägare kopplat till objektägare. Processen förklaras i texten ovan.

4.6 Dokumentation av informationssäkerhet

Informationssäkerhet ska vara en naturlig del av de komponenter som ingår i ett pm3-objekt. Säkerhetsförhållanden ska vara dokumenterade, och planerade säkerhetsåtgärder ska ingå i objektplanen så att de formellt fastställs gemensamt av objektägare verksamhet och objektägare it.

Säkerhetshöjande åtgärder utöver de behov som kan relateras till informationssäkerhethandboken ska finnas med i respektive objekts objektplan. Mål och

åtgärder kan uppkomma eller motiveras av t.ex. resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

ID	Regler och anvisningar för informationssäkerhet i objektplaner
V 6.1 0 1 2 3	Mål och åtgärder som kan relateras till informationssäkerhet ska finnas med i respektive objektplan.

4.6.1 Dokumenterade säkerhetsförhållanden

Ett objekts säkerhetsförhållanden ska dokumenteras. En sådan beskrivning ska finnas för varje relevant it-komponent (it-system/it-tjänst).I dokumentationen ska följande framgå:

- informationsmängder och informationstyper i it-system samt hur dessa är klassade (se kapitel 4.7)
- it-systemets/it-tjänstens skyddsnivå (se kapitel 4.7)
- planerade och genomförda riskanalyser samt resultat av dessa (se kapitel 4.8)
- behörighetshantering och loggning (se kapitel 4.9)
- ändringshantering (se kapitel 4.10)
- användarinstruktioner beträffande säkerhet (se kapitel 4.11)
- incidenthantering samt inträffade incidenter med referenser till incident-rapporter (se kapitel 4.12)
- kontinuitetshantering (se kapitel 4.13).

ID	Regler och anvisningar för objektsäkerhetsbeskrivning
V 6.2 0 1 2 3	Objekt och it-system/it-tjänster ska ha en systemsäkerhetsbeskrivning där objektet eller systemets informationssäkerhet är dokumenterad.

4.7 Informationsklassning

Informationsklassning innebär att information klassas i olika nivåer utifrån vad konsekvensen skulle kunna bli om informationen

- röjs till obehörig (konfidentialitet)
- inte är korrekt eller aktuell (riktighet)
- inte finns att tillgå när den behövs (tillgänglighet)
- inte är spårbar (spårbarhet).

För att ge stöd åt vilka omständigheter som avses är konsekvenserna indelade i ett antal nivåer – lindrig, måttlig, betydande, allvarlig eller synnerligen allvarlig konsekvens. Synnerligen allvarlig konsekvens redovisas inte i handboken eftersom denna konsekvensnivå inte relaterar till kommunen och dess verksamhet. Synnerligen allvarlig konsekvens relaterar till konsekvenser som avser Sveriges (rikets) säkerhet. Samtliga konsekvenser utom synnerlig allvarlig finns definierade i kapitel 3.7.4 – Kommunens konsekvenstabell.

Konsekvenserna bedöms för varje aspekt av informationssäkerhet, dvs. konfidentialitet, riktighet, tillgänglighet samt spårbarhet, vilket är detsamma som att tilldela informationen dess informationsklass.

Utifrån den klassning som görs finns skyddsåtgärder kopplade till respektive informationsklass. Exempelvis ska medarbetare som hanterar pappersinformation som kan leda till allvarliga konsekvenser om den röjs till obehörig alltid skydda informationen när den inte används genom att låsa in den i säkerhetsskåp.

Det finns en mängd skyddsåtgärder som är kopplade till regler och anvisningar för medarbetare, LKDATA samt faciliteter. (Se kapitel 2 – Informationssäkerhet för medarbetare, kapitel 5 – Informationssäkerhet i it-nära förvaltning och kapitel 6 – Informationssäkerhet och fysiskt skydd för detaljerade beskrivningar av skyddsåtgärder.)

Skyddsåtgärderna ska alltid utformas i paritet med den eventuella konsekvens som kan uppstå om konsekvensen realiseras. Gör därför realistiska värderingar för att undvika att information får onödigt högt skydd, med höga kostnader som följd, eller för lågt skydd, vilket medför för stor riskexponering.

Observera att man i värderingen aldrig ska bortse från kostnader bara för de kan anses höga. Informationsägarna ska endast uttrycka skyddsbehovet genom klassningen, även om detta kan medföra höga kostnader. Vid klassningen ska informationsägaren alltså bortse från kostnader för skyddsåtgärder. Dock ska värderingen av kostnader alltid bedömas i relation till risker. I kommunen är den övergripande riskägaren alltid ytterst kommundirektören. Det är hen som ytterst tar beslut och motiverar de kostnader i förhållande till verksamheters risker som indirekt härrör från en klassning. Läs mer i kapitel 4.7.5 – Vikten av att tilldela lämpliga informationsklasser.

4.7.1 Ansvar för att informationsklassning sker

Informationsägaren är ansvarig för att informationsklassning utförs för verksamhetens information och att detta dokumenteras i verksamhetens informationshanteringsplan (IHP) och kompletterande lista över arbetsmaterial.

Även om informationsägaren själv inte deltagit vid klassningstillfället beslutar hen slutgiltigt om klassningen av de informationstyper som redovisas i IHP. IHP ska tas upp för beslut i respektive nämnd.

Ansvar för informationsklassning		Fördjupad information
●	Informationsägaren är ansvarig för att informations- klassning utförs för verksamhetens information och att detta dokumenteras i verksamhetens informationshanteringsplan (IHP) och komplett-erande lista över arbetsmaterial.	Kapitel 3.6 – Informationsklass-ningens grunder Kapitel 3.7 – Informationsklassning i Linköpings kommun
●	Informationsägaren ansvarar för att informationsklassningen stämmer överens med de faktiska konsekvenserna för verksamheten.	Kapitel 3.3.5 – Informationsägare Kapitel 4.4 – Informationsägare

Nedan redogörs för åtta steg som vidtas före, under respektive efter en informationsklassning.

4.7.2 Före informationsklassningen

1. Om informationstyper inte har identifierats ska detta utföras först. Olika metoder kan användas, t.ex processkartläggning. Stadsarkivet kan också bistå med metodstöd.
2. De allmänna handlingar som verksamheten hanterar definieras och dokumenteras i IHP. Arbetsmaterial definieras och dokumenteras i kompletterande förteckning över arbetsmaterial.
3. Informationsägaren eller informationsägarbiträdet kallar till möte med medarbetare som har god kunskap och erfarenhet av informationshantering i verksamheten, så att samtliga konsekvenser kan bedömas tillförlitligt och väl avvägda.

4.7.3 Under informationsklassningen

Använd Mall för informationsklassning (se kapitel 7.2.1 – Stöddokument till informationssäkerhetshandboken) som komplement till redovisande planer.

4. Följande frågor besvaras för respektive informationstyp:
    - Vilka blir konsekvenserna om informationen/handlingen röjs till obehöriga (konfidentialitet)? Bedöm nivå på respektive konsekvens enligt konsekvenstabellen i kapitel 3.7.4.
    - Vilka blir konsekvenserna om informationen/handlingen är felaktig eller inaktuell (riktighet)? Bedöm nivå på respektive konsekvens enligt konsekvenstabellen i kapitel 3.7.4.
    - Vilka blir konsekvenserna om behöriga inte får tillgång till informationen/handlingen (tillgänglighet)? Bedöm nivå på respektive konsekvens enligt konsekvenstabellen i kapitel 3.7.4.

- Vilka blir konsekvenserna om informationen/handlingen inte går att spåra (spårbarhet)? Bedöm nivå på respektive konsekvens enligt konsekvenstabellen i kapitel 3.7.4.

5. Med hjälp av konsekvenstabellen klassas respektive informationssäkerhets-aspekt och informationstyp, vilka sedan dokumenteras i IHP respektive -kompletterande förteckning över arbetsmaterial.

6. En informationstyp (allmän handling eller arbetsmaterial) kan med fördel delas upp i två eller flera typer, om olika nivåer av konsekvenser är tänkbara beroende på innehåll. Detta är dock endast intressant om det hanteringsmässigt eller lagringsmässigt går att dela på informationen i verksamheten och på lagringsplatsen.

Informationsägaren ska söka relevant kompetens Om informationsägaren är osäker i sin bedömning av eventuella konsekvenser för verksamhet respektive individer ska hen söka stöd från relevant kompetens, t.ex. juridikenheten, säkerhetsenheten eller LKDATA.

4.7.4 Efter informationsklassningen

7. Berörda medarbetare informeras av informationsägaren om vilken klassning de olika handlingarna och informationstyperna fått, så att alla kan följa hanteringsreglerna i kapitel 2 – Informationssäkerhet för medarbetare.

8. Resultatet från informationsklassningen registreras i IHP och kompletterande lista över arbetsmaterial och delges till berörda objektägare verksamhet och resursägare samt till informationssäkerhetssamordnaren. Objekt-ägare verksamhet, objektägare it och resursägare tar sedan vid och ser till att informations-typer (allmänna handlingar och arbetsmaterial) tilldelas och upprätthåller ett relevant skydd (lämplig skyddsåtgärd).

9. Aktiviteten avslutas.

4.7.5 Vikten av att tilldela lämpliga informationsklasser

När en informationstyp klassas är det viktigt att bedöma konsekvenserna så verklighetsnära som möjligt. Informationsägaren ska alltid bedöma den värsta tänkbara konsekvensen för verksamheten i samtliga fyra informationssäkerhets-aspekter. Om informationstypen tilldelas en för låg klass, kan det resultera i att informationstypen inte får det skydd den behöver. En juridisk konsekvens som medvetet har värderats för lågt kan exempelvis leda till att en förvaltning medvetet bryter mot lagar och förordningar. Om en informationstyp tilldelas en för hög klass, kan det medföra onödiga kostnader för kommunen eftersom informationstypen får ett skydd den inte är i behov av.

Vilket skydd informationen behöver eller eventuellt kommer att få ska aldrig övervägas vid själva klassningen. Det är resursägarens (t.ex. objektägare it) ansvar att bedöma ett lämpligt skydd utifrån klassningen.

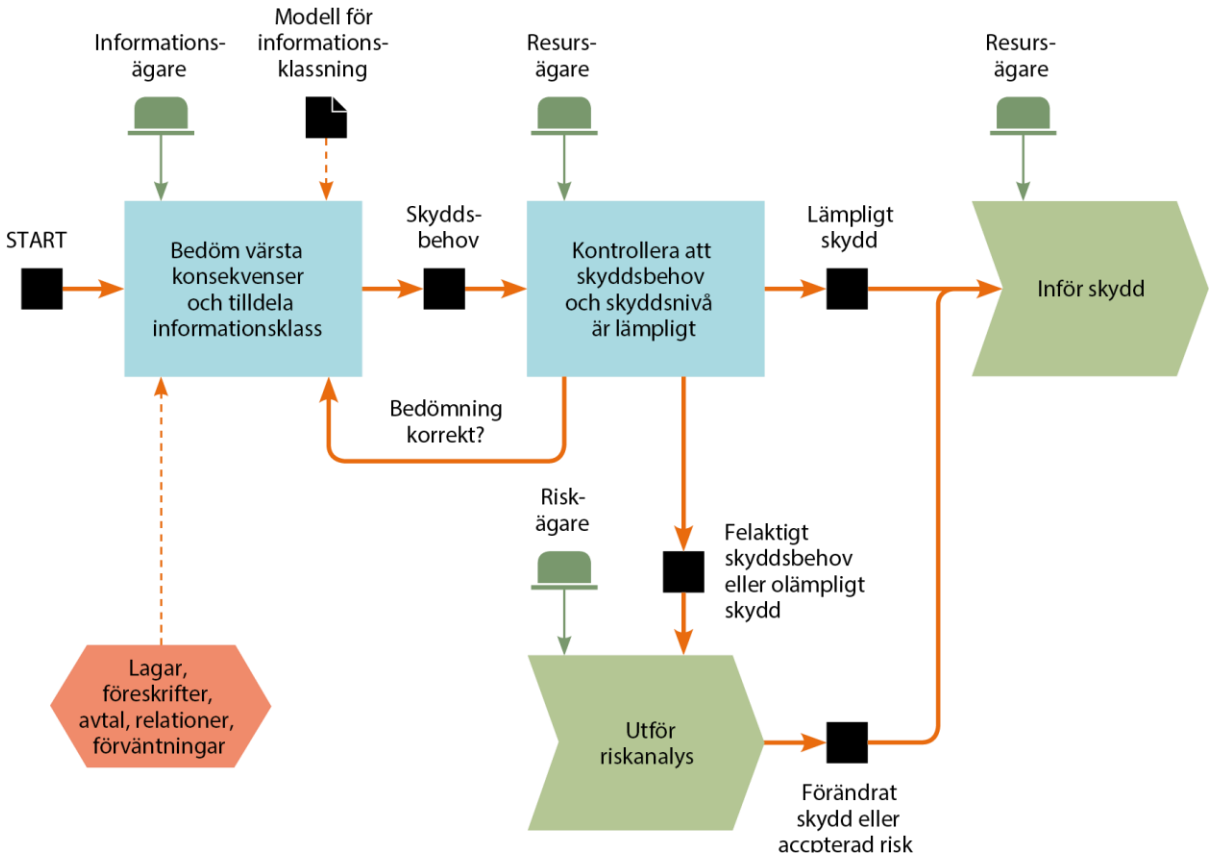
Avvikelser mellan klassning och skyddsnivå
I texten ovan diskuteras att informationsägaren endast ska utgå från verksamhetens behov av skydd för informationen utan att snegla på skyddsåtgärder vid bedömningen. Detta för att beskrivningen av skyddsbehovet ska bli korrekt.

I vissa situationer kan det finnas motiv att välja andra skyddsåtgärder än de som skyddsbehovet anger. Ett skäl kan vara ekonomi: Det kan vara för kostsamt att införa de skyddsåtgärder som klassningen beskriver. Om ett sådant beslut behöver tas ska ärendet vidarebefordras till informationssäkerhetsrådet för hantering.

I undantagsfall kan en annan skyddsnivå godkännas av kommundirektör. Dessa godkännanden kan vara tidsbegränsade. Observera att detta aldrig påverkar klassningen – den ska alltid ligga fast och beskriva verksamhetens verkliga konsekvenser vid en skada för informationen oavsett om en annan skyddsnivå godkänns. Avvikelser mellan klassningen och vald skyddsnivå ska registreras som en risk och tilldelas en riskägare.

Om informationsägaren låter skyddsnivåer styra klassningens resultat kommer processen för att värdera verksamhetens risker att kortslutas. Det är resursägarens ansvar att återkoppla till informationsägaren. Om resursägaren anser att en risk föreligger i förhållande till klassningsresultatet, eller om det finns något annat skäl för en översyn, ska en återkoppling till informationsägaren alltid ske. Det är extremt viktigt att hålla fast vid denna rollfördelning och

uppdelning av vem som ansvarar för respektive bedömning, så att inte information tilldelas felaktiga skyddsnivåer och information därmed får fel skydd.



Figur 27. Visar en förenklad processkarta över rollfördelning vid klassning, införande av skydd och bedömning av risker. Denna process förklaras i texten ovan och under.

Är informationsägare och resursägare inte överens vad gäller skyddsnivå eller skyddsbehov förs ärendet vidare till informationsäkerhetsrådet för ett utlåtande. Under tiden ett utlåtande förbereds i informationssäkerhetsrådet är det inte tillåtet att driva ärendet vidare. Detta utlåtande kan även föras vidare till kommundirektören för hantering, beroende på ärendets art. Den övergripande riskägaren i kommunen är alltid i sista hand kommundirektören. I vissa fall ska även informationsägande nämnd involveras.

Problem med införande av en skyddsnivå
Även om informationsägaren aldrig ska ta hänsyn till en specifik skyddsnivå så kan det i undantagsfall finnas situationer när en viss skyddsnivå bedöms medföra problem för verksamheten. Exempelvis kan det handla om att skyddet bedöms kräva kraftigt ökad arbetsbörda eller att kostnader för skyddet bedöms som orimliga.

Innan informationsägaren eskalerar ett ärende av denna typ ska alternativa åtgärder alltid övervägas. Ibland kan denna typ av situationer lösas genom att informationstypen som avses delas upp i flera ytterligare typer så att skyddsbehovet förändras. Ytterligare en alternativ åtgärd är att kontrollera om någon del av innehållet i typen kan utelämnas för att skyddsbehovet ska förändras – detta förfarande är exempelvis vanligt vid hantering av personuppgifter.

ID	Regler och anvisningar för att klassa information
V 7.1 0 1 2 3	Informationstyper i verksamheten ska inventeras, dokumenteras och klassas enligt kommunens modell för informationsklassning.
V 7.2 0 1 2 3	Berörda i verksamheten ska informeras om vilken klassning informationstyperna har tilldelats, så att reglerna för hantering kan följas.
V 7.3 0 1 2 3	Objektägare verksamhet ska informeras om skyddsbehov eller motsvarande informationsklassning för aktuell informationstyp.
V 7.4 0 1 2 3	Informationsägaren ska se till att alla konsekvensbedömningar är verklighetsnära så att informationsklassningen uttrycker ett lämpligt skyddsbehov.

4.8 Riskanalys

Vid en riskanalys står informationen i fokus utifrån dess utsatthet vad gäller konfidentialitet, riktighet, tillgänglighet och spårbarhet. Analysen identifierar och bedömer scenarion med verkliga eller fiktiva händelser som påverkar informationen, t.ex. att information sprids till obehöriga personer, att informationen ändras obehörigt, att informationen inte kan nyttjas inom rimlig tid eller att informationen inte kan användas över huvud taget.

Till skillnad från en informationsklassning tar en riskanalys också hänsyn till sannolikheten för olika händelser och aktuella skydd för informationssäkerhet.

Ansvar för utförande av riskanalyser		Fördjupad information
●	Alla medarbetare med en utpekad informationssäkerhetsroll ansvarar för att initiera riskanalyser när de vet eller har skäl att anta att ett gap existerar mellan informationsägarens skyddsbehov (önskat läge) och det faktiska skydd som införts (nuläge).	Kapitel 3.8 – Risker och hantering av risker

En riskanalys innebär att man identifierar hot och brister samt värderar sannolikheten för att de förverkligas och konsekvenserna om de förverkligas. Den omfattar följande steg:

- Identifiering av risker: Vilka risker utsätts vi för?
- Värdering av risker: Vilken är sannolikheten och vilka blir konsekvenserna?
- Hantering av risker: Ska vi åtgärda eller acceptera?

En riskanalys ger en ögonblicksbild av situationen med hänsyn till alla aktuella faktorer. Analysen ger ett underlag för beslut om åtgärd eller acceptans av risk. Över tid ändrar sig förutsättningarna och riskanalysen behöver uppdateras eller göras om.

Riskanalyser ska alltid genomföras när det existerar ett gap mellan behov av skydd och det faktiska skyddet, (se kapitel 3.6 – Informationsklassningens grunder). Andra situationer som kan aktivera behovet av en riskanalys är vid

- förändrad verksamhet, t.ex. omorganisation, flytt, större förändrad användning eller ändrad hantering av informationstyper
- start av projekt där värdefull information kan komma att hanteras
- behov av ett underlag för kontinuitetsplaner
- förändrad användning av it-system
- upphandling av nya it-system
- större förändringar gällande vilka medarbetare som har tillgång till en viss informationstyp
- utredning gällande avsteg från krav under informationsklassning
- andra situationer när det kan förväntas att riskerna förändras.

4.8.1 Inför en riskanalys

För att kunna genomföra en lyckad riskanalys är det viktigt att rätt kompetenser finns med i arbetet. Kunskap om det område (t.ex. ett projekt, en process eller en tjänst) som riskanalysen ska omfatta är viktigt. Det ska ingå representanter med förståelse för hur värdefull den berörda informationen är för verksamheten samt personer som dels har erfarenhet av att bedöma sannolikheter för olika konsekvenser, dels kan föreslå lämpliga åtgärder för att minimera risker.

Om man är osäker på hur en riskanalys ska genomföras är det bra om någon med erfarenhet av arbete med informationssäkerhet leder eller deltar i analysarbetet.

Beroende på omfattning av riskanalysen kan det vara lämpligt att dela upp arbetet i flera steg. Det ökar också möjligheten att ta in lämplig kompetens för att bedöma riskhantering för specifika resurser (exempelvis om ingående kompetens krävs för ett specifikt it-system).

4.8.2 Riskidentifiering

En lämplig inledning på en riskanalys är en övning där deltagarna får tänka fritt (s.k. brainstorming) om tänkbara scenarion i den verksamhet, process, funktion eller information som riskanalysen omfattar.

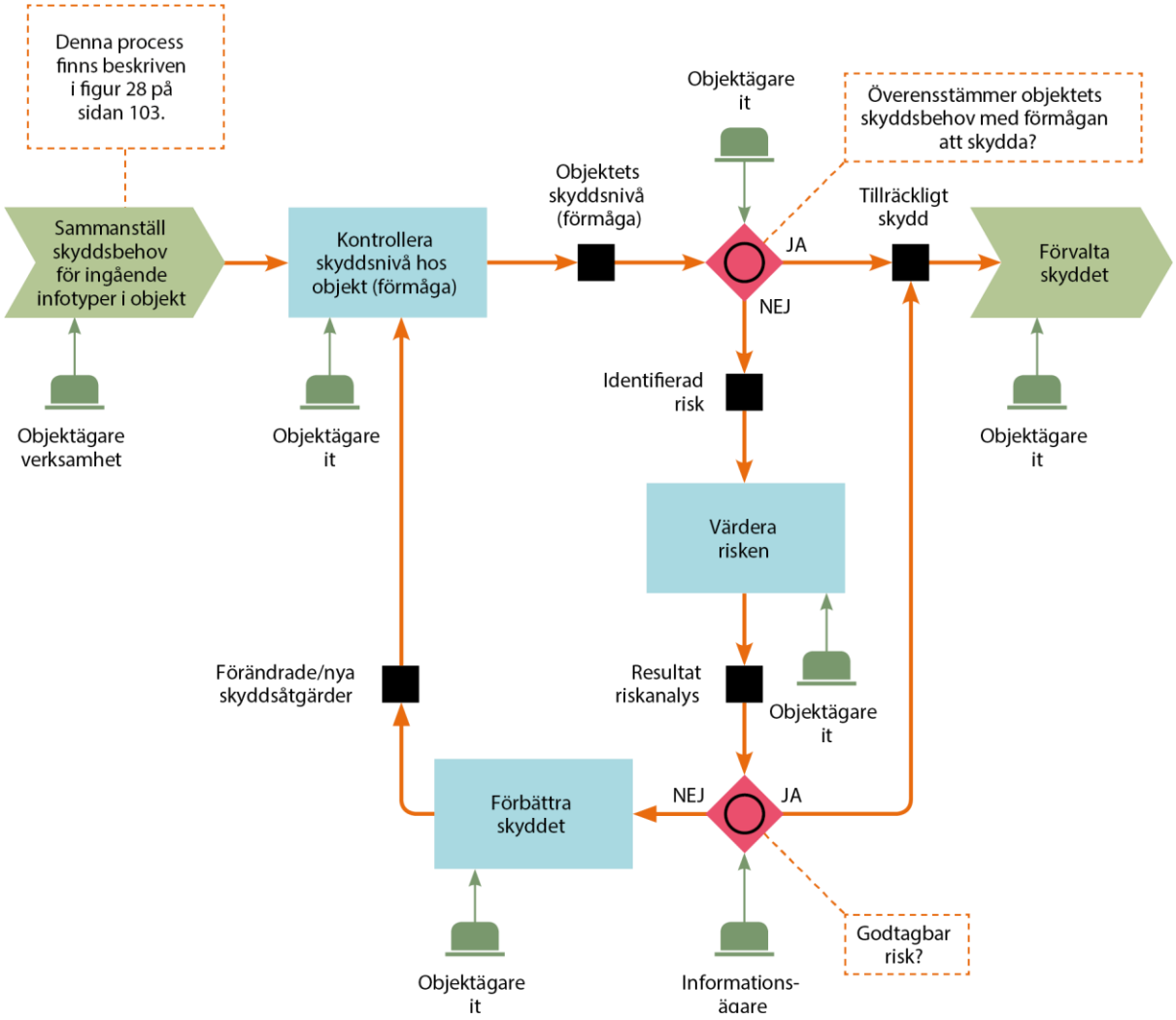
4.8.3 Riskvärdering

Varje scenario värderas utifrån vilka konsekvenser det får för verksamheten om scenariot realiseras och sannolikheten att scenariot inträffar (riskvärdering). För bedömningen används mallar som har koppling till de konsekvensnivåer som finns i kapitel 3.7.4 – Kommunens konsekvenstabell. Det är viktigt att använda en gemensam bedömningsskala för att kunna jämföra risker med varandra.

Befintlig informationsklassning är till hjälp när man bedömer konsekvenser. Att samla in sådan information ingår därför i förberedelserna.

Sannolikhet bedöms utifrån erfarenhet, exempelvis om liknande fall har inträffat tidigare. Här kan kunskap om informationssäkerhetsincidenter vara bra, liksom omvärldsbevakning och kunskap om it-säkerhet. Även det skydd som redan finns implementerat för informationen påverkar. Exempelvis ökar sannolikheten för att ett hot ska realiseras om skydd saknas eller är undermåligt. När det gäller sabotage av olika slag är motivet en viktig faktor att överväga.

Det är viktigt med en bra beskrivning av varje scenario. Orsak och verkan bör beskrivas. Det gör det möjligt att förstå hur eventuella åtgärder kan minska riskerna.



Figur 28. Processbeskrivning över riskanalys inom informationssäkerhetsarbetet. Processbeskrivningen visar via en ruta att objektsägaren sammanställer skyddsbehov för ingående infotyper i ett objekt. Detta går sedan vidare för kontroll av skyddsnivån hos objektägare i detta fall IT. Detta går sedan vidare till en annan ruta, där man ser över om objektetsskyddsbehov överensstämmer med förmågan att skydda. Om svar Ja förvaltas skyddet, om svar nej ska risken identifieras och värderas. Är risken godtagbar förvaltas den. Om Nej, förbättras skyddet och går åter tillbaka i processen för kontroll.

Bild: Bilden visar ett kontorslandskap med stolar, bord och datorer. en person sitter med ryggen emot.

Exempel
Om den information som ett hot riktas mot är klassad med höga skyddsbehov blir konsekvensen allvarlig om informationen går förlorad. Därför är det bra att känna till informationsklassningen för den information som riskanalysen troligen kommer att handla om.

4.8.4 Riskhantering

När riskerna är värderade utses en riskägare, vilken oftast även är informationsägare och den vars verksamhet blir drabbad om hotet realiseras. Riskägaren kan besluta huruvida en risk ska accepteras eller åtgärdas. I normalfallet kan obetydliga risker accepteras medan man bör överväga att behandla förhöjda risker. Höga och mycket höga risker ska alltid hanteras. Om en risk accepteras av riskägaren ska riskacceptansen motiveras i riskanalysens dokumentation.

Ibland kan vissa risker behöva vidarebefordras till informationssäkerhetsrådet för utlåtande, se även kapitel 4.7.5 – Vikten av att tilldela lämpliga informationsklasser.

De alternativ som finns utöver att acceptera en risk är att

- minska risken – införa en ny eller förstärka befintlig skyddsåtgärd
- undvika risken – ta bort själva området där risken kan uppstå
- flytta risken – t.ex. försäkra mot kostnader som kan uppstå om risken realiseras.

Risker där konsekvensen är mycket hög men sannolikheten är extremt låg hanteras vanligtvis genom kontinuitetsplanering och krishantering.

Vid en minskning av risk ska lämpliga skyddsåtgärder fastställas. Vid en riskanalys med fokus på informationssäkerhet kan åtgärderna vara

- organisatoriska – t.ex. en förbättrad rutin, medvetenhetsutbildning eller en tydligare regel
- tekniska – t.ex. skydd av ett it-system, ett nätverk eller larm och lås.

Målet är att helt eller delvis förhindra negativ påverkan från risken genom att minska sannolikheten att risken ska inträffa eller minska konsekvensen när den inträffar.

4.9 Behörighetshantering och loggning

För att få behörighet till olika it-system eller information måste användare först identifieras. Det görs ofta genom att koppla användares identitet till ett unikt inloggningskonto. Inloggning innebär att användaren identiferar sig (autentiseras) med lösenord eller på andra sätt. Efter inloggning kan användaren få tillgång till olika resurser beroende på behörigheter som har kopplats till kontot. Även fysiska skydd kan användas för att begränsa obehörig åtkomst, se kapitel 6 – Informationssäkerhet och fysiskt skydd.

Gruppkonton får bara användas i undantagsfall och ska då uppfylla kraven i kapitel 5.4 – Styrning av åtkomst.

Behörigheten ska baseras på den information en användare behöver för att utföra sina arbetsuppgifter (s.k. need to know). En bra förutsättning för rätt behörighetstilldelning är att informationen är strukturerad och klassad.

Exempel
Inom vissa områden, t.ex. vård och omsorg, kan akuta situationer innebära att vissa medarbetare behöver behörighet till en stor mängd information om brukare eller patienter, utöver den information de normalt behöver. I dessa fall hanteras åtkomst till information genom regler (s.k. regelstyrd åtkomst/behörighet). Dessa regler kan innebära att medarbetaren får ta del av information som inte gäller dennas ordinarie arbetsuppgifter. Regelstyrd åtkomst/behörighet ska alltid kompletteras med funktioner för analys och uppföljning av loggar för att upptäcka och minska otillåten användning.

Behörighet och åtkomst till information kan även vara tekniskt styrd (s.k. teknikstyrd åtkomst/behörighet). I dessa fall är medarbetaren tekniskt begränsad att ta del av information genom ett behörighets- och kontrollsystem (BKS). Med teknikstyrd åtkomst/behörighet kan medarbetaren inte ta del av information hen inte är behörig till.

Ansvar för behörighetshantering och loggning		Fördjupad information
●	Informationsägare och objektägare verksamhet kan besluta om vilka behörighetsprinciper som ska gälla.	

Informationsägare och objektägare verksamhet kan besluta om vilka behörighets-principer som ska gälla.

Uppföljning och kontroll av att rätt användare har rätt behörigheter ska ske minst en gång per år av dem som beslutat om behörigheterna. För användare med särskilda behörigheter (administratörer) ska revision ske minst varje halvår.

När medarbetare med särskilda behörigheter slutar eller byter tjänst ska det finnas rutiner som direkt hanterar dessa administratörers behörigheter.

För externa användare, exempelvis konsulter, gäller samma regler för åtkomst och tilldelning som för kommunens anställda. För externa användare ska åtkomsten även vara tidsbegränsad (högst ett år i taget) för den tid som krävs för att utföra uppgiften samt föregås av en signering av blankett för tystnadsplikt.

Det ska finnas rutiner för underhåll och förvaltning av behörigheter till it-komponenter som beskriver hur man beställer, ändrar eller tar bort behörigheter. Dessa rutiner ska vara kopplade till både den it-nära och den verksamhetsnära förvaltningen, så att behörighetsförändringarna kan genomföras skyndsamt. Förändringar i användares behörigheter ska dokumenteras med ansvarig för beslutet och själva förändringen, så att det framgår över tid vem som har haft behörighet till vad.

4.9.1 Logghantering

Samtliga it-system bör övervakas och loggas vad det gäller användaraktiviteter, avvikelser, fel och händelser som rör informationssäkerhet, för att öka spårbarheten och möjliggöra incidentutredningar samt upptäcka avvikelser från lagkrav eller interna regelverk. Detta är obligatoriskt om it-system/it-tjänster hanterar information med förhöjda eller höga skyddsbehov eller om regelstyrd

behörighetshantering används. Regelstyrd behörighetshantering innebär att en användare har tillgång till mer information än hen har rätt till, för att användaren i exempelvis en akut situation behöver information som hen normalt inte har rätt till. I viss verksamhet styrs detta av lag som i vissa fall ger utökade befogenheter.

När loggning används ska det finnas processer eller rutiner för dess hantering. Dessa ska innefatta

- hur loggning går till
- hur loggar skyddas mot manipulation och obehörig åtkomst
- hur länge loggar sparas
- hur loggar granskas.

Kan logginformationen knytas till en enskild person är informationen att betrakta som personuppgifter och omfattas då av dataskyddsförordningen.

Processer och rutiner för loggning ska följas upp av informationsägare eller objektägare verksamhet.

ID	Regler och anvisningar för behörighetshantering och loggning
V 9.1 0 1 2 3	Det ska finnas en dokumenterad rutin för hantering av behörigheter till it-komponenter beställning, ändring och borttag.
V 9.2 0 1 2 3	Rutiner för behörighetshanteringen ska följas upp av informations-ägare och objektägare verksamhet.
V 9.3 0 1 2 3	Varje användare ska ha ett unikt inloggningskonto.
V 9.4 0 1 2 3	Externa användares åtkomst ska vara tidsbegränsad (högst ett år) samt föregås av blankett för tystnadsplikt.
V 9.5 0 1 2 3	Det ska finnas dokumenterade rutiner för logghantering i objekt.
V 9.6 2 3	Förhöjda eller höga skyddsbehov på konfidentialitet, riktighet eller tillgänglighet innebär höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk.
V 9.7 0 1 2 3	Loggning av användares aktiviteter är obligatorisk när regelstyrd behörighetshantering används i stället för teknisk behörighetshantering.
V 9.8 0 1 2 3	Förändringar i anställningar och roller ska omedelbart rapporteras till både den it-nära och den verksamhetsnära förvaltningen, så att reglering kan ske skyndsamt.
V 9.9 0 1 2 3	Ansvariga för tilldelning av behörigheter ska kontrollera användare och deras behörigheter minst en gång per år. För användare med administrativa behörigheter ska kontroll ske minst en gång per halvår.
V 9.10 0 1 2 3	Informationsägare ställer krav på rutiner för loggkontroller. Objektledare verksamhet ansvarar för genomförande.

4.10 Ändringshantering

Ändringar i it-system/it-tjänster ska ske enligt Linköpings kommuns förvaltningsmodell. Det innebär att ändringar ska ske strukturerat – dels för att säkra it-systemets/it-tjänstens säkerhet, funktionalitet och användbarhet, dels för att minimera antalet fel orsakade av förändringen.

Ansvar för ändringshantering		Fördjupad information
●	Informationsägare och objektägare verksamhet kan besluta om vilka behörighetsprinciper som ska gälla.	

Ändringar i it-system/it-tjänst ska samordnas med change managementprocessen inom den it-nära förvaltningen. Större förändringar i eller kring it-system/it-tjänst ska föregås av en riskanalys.

It-system/it-tjänst ska avvecklas strukturerat i samråd med Stadsarkivet så att dess information hanteras korrekt.

ID	Regler och anvisningar för ändringshantering
V 10.1 0 1 2 3	Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i it-system/it-tjänst.
V 10.2 0 1 2 3	Vid avveckling av it-system/it-tjänst ska en plan upprättas i samråd med Stadsarkivet för hur information ska migreras, gallras eller slutarkiveras.

4.11 Användarinstruktioner

Objektägare verksamhet ansvarar för att det finns användarinstruktioner för samtliga användare av it-system/it-tjänst. Användare ska utbildas enligt instruktionerna och objektägaren kontrollerar att instruktionerna följs.

Ansvar för användarinstruktioner		Fördjupad information
●	Objektägare verksamhet är ansvarig för att användarinstruktioner framställs.	Kapitel 4.2 – Verksamhetsnära roller och ansvar.

Användarinstruktionerna ska omfatta följande delar av informationssäkerhet:

- regler kring inloggning och lösenordshantering behörigheter
- särskilda instruktioner för hur information med sekretess och stark -sekretess ska hanteras, t.ex. känsliga eller skyddade personuppgifter
- information om vad som loggas
- konsekvenser av att bryta mot användarinstruktioner, t.ex. att ta del av eller sprida information med stark sekretess.
- incidentrapportering, där användare ska vara vaksama på brister och
- incidenter i it-systemet/it-tjänsten och veta hur man ska rapportera dessa

  (se kapitel 4.12 – Incidenthantering).

Användare är även skyldiga att följa samtliga regler och anvisningar i kapitel 2 – Informationssäkerhet för medarbetare.

ID	Regler och anvisningar för användarinstruktioner
V 11.1 0 1 2 3	Informationssäkerhetsregler ska finnas med i användarinstruktioner.
V 11.2 2 3	Det ska finnas särskilda instruktioner för hantering av information med **sekretess** och **stark sekretess** som t.ex. skyddade personuppgifter.

4.12 Incidenthantering

Incidenter som kan relateras till informationssäkerhet är oönskade händelser som kan, eller skulle ha kunnat, leda till att informationens konfidentialitet, riktighet, tillgänglighet eller

spårbarhet påverkas negativt. Objektägare verksamhet och informationsägare ansvarar för att sådana incidenter hanteras, sammanställs, dokumenteras och rapporteras enligt rutin som informationssäkerhetssamordnaren anvisar.

Ansvar för incidenthantering		Fördjupad information
●	Objektägare verksamhet och informationsägare ansvarar för att incidenter hanteras, sammanställs, dokumenteras och rapporteras enligt rutin som informationssäkerhetssamordnaren anvisar.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.11 – Incidenthantering

Alla informationssäkerhetsrelaterade incidenter ska rapporteras

Alla typer av informationssäkerhetsrelaterade incidenter ska rapporteras enligt rutin som informationssäkerhetssamordnaren anvisar. Vissa typer av incidenter ska även rapporteras till andra instanser, t.ex. personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY) och dataskyddsombud (DSO), fysiskt inbrott till säkerhetschefen och dataintrång till MSB. Som informationssäkerhetsrelaterade incidenter inom kommunen räknas:

- informationssäkerhetsincidenter
- personuppgiftsincidenter
- it-säkerhetsincidenter
- fysisk säkerhetsincidenter.

Informationssäkerhetsincidenter som gäller it kan delas in i mindre incidenter och allvarliga incidenter.

- Mindre incidenter är när få medarbetare blir drabbade vid t.ex. mindre tekniska fel i system eller när enstaka användare inte följer användarinstruktionerna. I systemets användarinstruktioner ska det finnas rutiner för hur användare ska rapportera mindre incidenter (se även kapitel 2.2 – Samtliga medarbetare har ansvar för informationssäkerheten). Rutiner för hur incidenter ska tas emot och hanteras ska finnas.
- Allvarliga incidenter kan vara exempelvis större störningar i ett it-system, ett längre avbrott (några timmar eller mer), dataintrång, en brand som förstör information eller infektion av skadlig kod. En allvarlig incident kräver en utredning som ska dokumenteras. Utredningen ska drivas av informationsägaren eller objektledaren i

samverkan med säkerhetsenheten och relevanta aktörer inom den it-nära förvaltningen.

Objektledare verksamhet ansvarar för att löpande uppdatera rapporterade -incidenter med genomförda åtgärder, kvarstående åtgärder och att incidenten är färdigbehandlad. Eventuella åtgärder som kvarstår ska hanteras i objektplaner.

ID	Regler och anvisningar för incidenthantering
V 12.1 0 1 2 3	Det ska finnas rutiner för hur användare ska rapportera informationssäkerhetsincidenter.
V 12.2 0 1 2 3	Akuta informationssäkerhetsincidenter ska åtgärdas skyndsamt.
V 12.3 0 1 2 3	Allvarliga informationssäkerhetsincidenter ska utredas och dokumenteras.
V 12.4 0 1 2 3	Incidenter ska rapporteras enligt rutin som informationssäkerhetssamordnaren anvisar. Observera att vissa typer av incidenter även ska rapporteras till andra instanser, t.ex. personuppgiftsincidenter till Integritetsskyddsmyndigheten och dataskyddsombud (DSO) och dataintrång till MSB.

4.13 Kontinuitetshantering

Många funktioner inom kommunen har krav på kontinuitet, inte minst inom informationshantering. Att system och tjänster är tillgängliga är avgörande för att en god kontinuitet ska kunna upprätthållas. Under informationsklassningen fastställs verksamhetens önskemål på tillgänglighet och lämpliga skyddsåtgärder införs sedan av berörda parter.

Ansvar för incidenthantering		Fördjupad information
●	Objektledare verksamhet ansvarar för att upprätta kontinuitetsplaner, vilka ingår som del av respektive verksamhets krisplan.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.12 – Kontinuitetshantering

Men oavsett vilka förebyggande skyddsåtgärder som finns kan avbrott ändå ske, och under vissa omständigheter kan beroendet av en viss funktion i ett it-system eller en it-tjänst vara så högt att ett avbrott aldrig kan tillåtas. I dessa fall måste verksamheten utarbeta egna kontinuitetsplaner för att kunna fullfölja sina åtaganden.

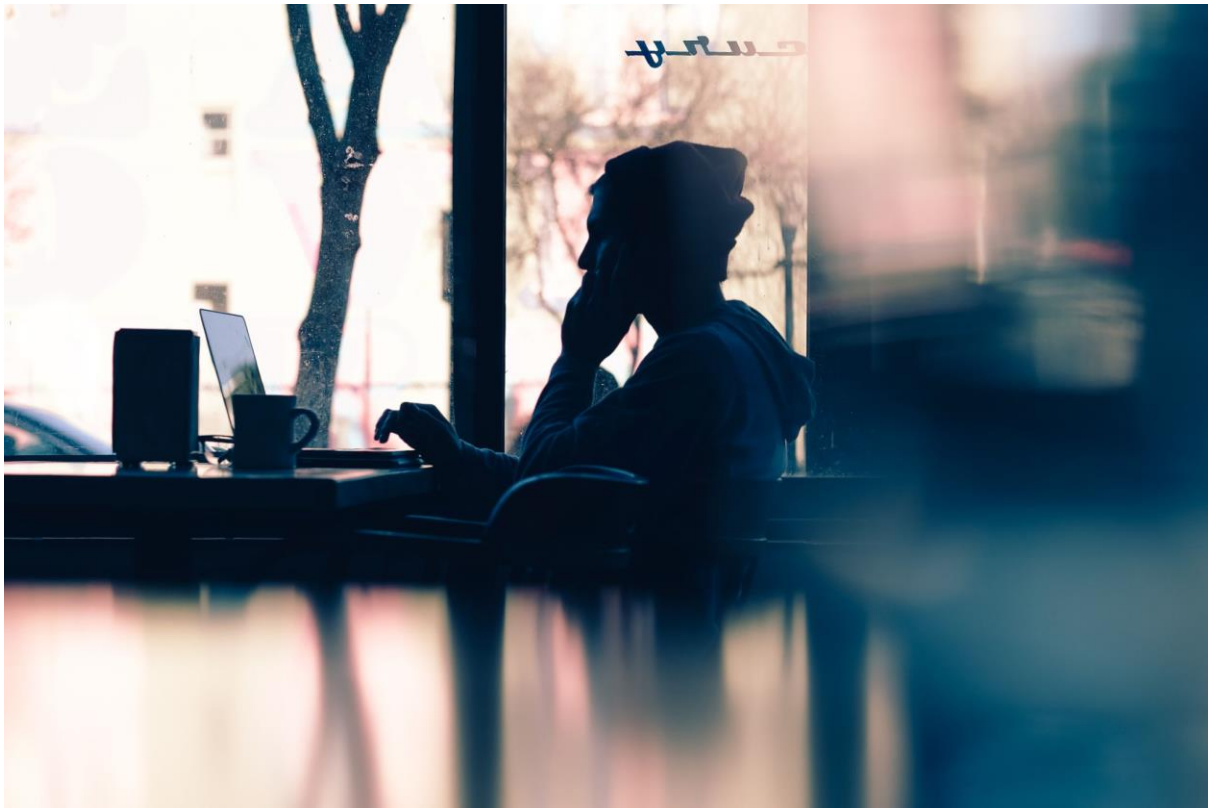
Beroende av nyckelpersoner ska undvikas. Om verksamheten är beroende av nyckelpersoner ska detta åtgärdas, t.ex. genom utbildning av ersättare.

Nyckelpersonsberoendet kan också minska genom användning av vedertagna standarder och standardprodukter.

Objektledare verksamhet ska upprätta kontinuitetsplaner, vilka ingår som en del av respektive verksamhets krisplan. Dessa ska användas vid större avbrott. Kontinuitetsplanerna ska innehålla ansvarsförhållanden, kontaktpersoner samt eskaleringsvägar till relevanta interna och externa aktörer. Samverkan ska ske med den it-nära förvaltningen.

ID	Regler och anvisningar för kontinuitetshantering
V 13.1 	Kontinuitetsplaner med manuella rutiner ska finnas för kritiska objekt med höga skyddsbehov gällande tillgänglighet.
V 13.2 	Beroende av nyckelpersoner ska undvikas och åtgärdas.
V 13.3 	Kontinuitetsplaner som upprättas inom verksamheten ska innehålla ansvarsförhållanden, kontaktpersoner och eskaleringsvägar.

Kapitel 5 -
Informationssäkerhet i it-nära förvaltning



5.1 Inledning

Detta kapitel riktar sig till den it-nära förvaltningen i Linköpings kommun samt till externa parter som arbetar med it-nära verksamhet på uppdrag av kommunen, exempelvis inhyrda konsulter.

Informationssäkerhet i it-miljön beskrivs ofta som it-säkerhet och innefattar skyddsåtgärder för olika resurser för informationsbehandling (it-komponenter) som molntjänster, system, databaser, verktyg och infrastruktur i form av hård- och mjukvara. Termen it-komponent används i detta kapitel som ett generellt samlingsbegrepp om ingen specifik hård- eller mjukvara avses.

Från kapitel 5.3 och framåt är kapitlet strukturerat utifrån motsvarande avsnitt i standarden SS-ISO/IEC 27002.

Kapitel		Motsvarande avsnitt i ISO/IEC 27002
5.3	Hantering av tillgångar	8
5.4	Styrning av åtkomst	9
5.5	Kryptering	10
5.6	Fysisk och miljörelaterad säkerhet	11
5.7	It-driftsäkerhet	12
5.8	Kommunikationssäkerhet	13
5.9	Anskaffning och utveckling av it-komponenter	14
5.10	Skyddskrav vid upphandling	15
5.11	Incidenthantering	16
5.12	Kontinuitetshantering	17
5.13	Granskning och kontroll	18

I standarden finns vägledningar och anvisningar, och den kan med fördel användas som ett stödjande dokument. Även andra standarder och vägledningar, från t.ex. Myndigheten för samhällsskydd och beredskap (MSB), kan vara ett stöd och komplement till denna handbok.

Informationsklassning är en central del av kommunens arbete med informationssäkerhet. Klassningen resulterar i att information kan ha grundläggande, förhöjda eller höga skyddsbehov vad gäller konfidentialitet, riktighet, tillgänglighet och spårbarhet enligt kommunens klassningsmodell (se kapitel 3.7.1 – Kommunens modell för informationsklassning för mer information).

Förslag till skyddsbehov omformas i nästa steg till skyddsåtgärder och kopplas till de it-komponenter som hanterar informationen. För förhöjda och höga skyddsbehov kan det

finnas kompletterande skyddsåtgärder. Skyddsbehoven markeras genomgående i kursiv stil för förhöjda skyddsbehov och i fetstil för höga skyddsbehov. Raderna i tabeller med regler och anvisningar har grafiska markeringar för att tydliggöra när reglerna/anvisningarna är tillämpliga.

5.2 It-nära roller och ansvar

Ansvaret för informationssäkerhet och it-säkerhet inom den it-nära förvaltningen följer med ordinarie verksamhetsansvar, t.ex. för infrastruktur. Det innebär att chefer och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av informations- och it-säkerhet för de processer och it-komponenter de ansvarar för.

Linköpings kommun har beslutat att tillämpa pm3:s modell för förvaltningsstyrning. Detta kapitel kompletterar förvaltningsstyrningen med regler och anvisningar om informationssäkerhet i den it-nära förvaltningen (se även ITIL).

5.2.1 Objektägare it och CIO

Objektägare it ansvarar för att it-säkerheten i samtliga it-komponenter i pm3 antingen i ett objekt eller som ett objekt är beroende av överensstämmer med verksamheternas informationsklassning, så att rätt skyddsnivå upprätthålls. CIO ansvarar för it-säkerheten i resterande it-komponenter.

Objektägare it och CIO ska för den it-nära förvaltningen dels ansvara för att regler och anvisningar i denna handboks följs, dels redovisa till objektägare verksamhet och till informationssäkerhetsrådet om det finns brister (risker) i förhållande till skyddsbehoven.

Objektägare it och CIO har också ett ansvar för att samtliga it-komponenter är identifierade och förtecknade samt förvaltas löpande.

Ansvar som objektägare it och CIO		Fördjupad information
●	Objektägare it ansvarar för att samtliga (inom pm3) it-komponenters skyddsnivåer överensstämmer med verksamheternas informationsklassning. CIO ansvarar för resterande it-komponenter.	Kapitel 5.3 – Hantering av tillgångar Kapitel 5.9 – Anskaffning och utveckling av it-komponenter

5.2.2 Objektledare it

Objektledare it samverkar med objektledare verksamhet och ansvarar för att rätt skyddsåtgärder implementeras i objekten utifrån beslutade objektplaner. Otillräckliga eller bristande skyddsåtgärder redovisas till objektägare it.

Ansvar som objektledare it		Fördjupad information
●	Objektledare it samverkar med objektledare verksamhet och ansvarar för att rätt skyddsåtgärder implementeras i objekten utifrån beslutade objektplaner.	Kapitel 5.3 – Hantering av tillgångar.

5.2.3 It-säkerhetssamordnare

It-säkerhetssamordnaren ansvarar för att samordna arbetet med säkerhet i alla it-komponenter och är stödjande vid kravställning på externa aktörer. It-säkerhetssamordnaren har däremot inte ansvar för it-komponenternas skydd utan ska stödja verksamheten och kontrollera att rätt skyddsåtgärder är applicerade på it-komponenterna. It-säkerhetsamordnaren rapporterar till objektägare it.

För it-säkerhetssamordnaren innebär arbetsuppgifterna i huvudsak att ansvar i tabellen nedan upprätthålls.

It-säkerhetssamordnaren ansvarar för att		Fördjupad information
●	följa upp och granska efterlevnaden av regler och anvisningar för it-säkerhet	Kapitel 2 – Informationssäkerhet för medarbetare
●	stödja vid utformning av regler och anvisningar för it-säkerhet	Kapitel 3.4 – Informations-säkerhetsorganisation
●	stödja objekten i it-säkerhetsfrågor	Kapitel 5.3 – Hantering av tillgångar

●	stödja och bevaka att handlingsplaner tas fram och genomförs för att åtgärda brister som konstaterats i samband med säkerhetsgransk-ningar eller riskanalyser	Kapitel 3.5 – Kommunens centrala dokument för styrning
●	bistå vid utredning av misstänkta och inträffade it-säkerhetsincidenter	Kapitel 5.11 – Incidenthantering
●	stödja olika objekt vid kravställning rörande it-säkerhet och uppföljning av leverantörers säkerhetsåtaganden	Kapitel 5.9 – Anskaffning och utveckling av it-komponenter
●	leda eller delta i riskanalys av it-säkerhets-relaterade risker	Kapitel 4.8 – Analys och hantering av risker
●	verka för ett höjt säkerhetsmedvetande inom it-verksamheten	Kapitel 2 – Informationssäkerhet för medarbetare
●	ta fram statusrapporter för kommunens it-säkerhet	Kapitel 3.5 – Kommunens centrala dokument för styrning

It-säkerhetssamordnaren arbetar nära kommunens informationssäkerhetssamordnare och ingår i kommunens informationssäkerhetsråd. It-säkerhetssamordnaren ska också omvärldsbevaka, nätverka och samverka externt inom området.

5.3 Hantering av tillgångar

5.3.1 Skydd av it-komponenter

Vilka skyddsåtgärder som ska finnas implementerade kring en it-komponent bestäms av skyddsbehovet (se även kapitel 3.7.5 – Klassningens resultat). Informationen med högst informationsklass (som hanteras av it-komponenten) avgör vilka skyddsåtgärder som ska finnas på plats.

Beroende på it-komponentens typ (molntjänst, system, databas, verktyg eller infrastruktur i form av hård- eller mjukvara) kopplas relevanta skyddsåtgärder till it-komponenten för att ge den information som hanteras i it-komponenten ett relevant skydd. Information om it-komponenter återfinns vanligen i en CMDB.

Flera icke-kritiska it-komponenter kan bli kritiska

Var uppmärksam på att flera it-komponenter som var för sig inte är kritiska kan bli kritiska tillsammans och kan kräva ytterligare skyddsåtgärder.

Andra aspekter än informationsklassningen kan göra att skyddsbehovet förändras, t.ex. om en it-komponent stödjer flera andra it-komponenter (tjänster eller system) som var för sig inte är kritiska men som tillsammans blir kritiska om de inte finns tillgängliga. Ytterligare skyddsåtgärder kan då implementeras för att skydda it-komponentens tillgänglighet. CIO och objektägare it tillsammans ansvarar för och hanterar sådan omvärdering av en it-komponents skyddsbehov.

I dokumentet It-tekniska säkerhetskrav gällande it-komponenter (se Linweb) återfinns detaljerade krav för respektive informationsklass. Informationsägare för dokumentet är CIO.

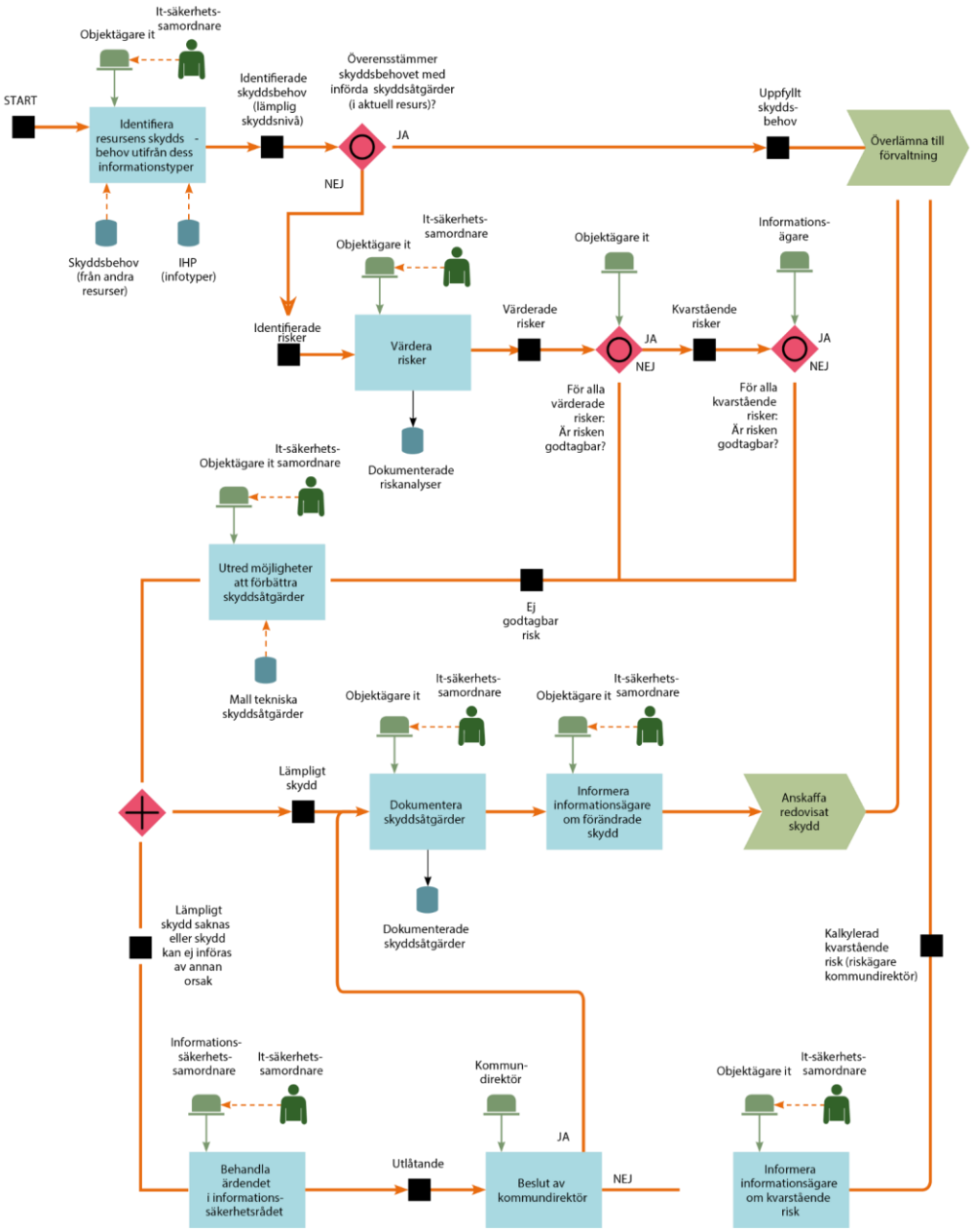
Flera it-tekniska säkerhetshöjande skyddsåtgärder sker vanligen genom det som brukar kallas härdning. När en it-komponent levereras är den vanligen inte anpassad till den miljö eller tillämpning som den ska användas i. Komponenten (datorn, operativsystemet, applikationen etc.) är snarare grundkonfigurerad att tillfredställa så många miljöer, tillämpningar och användningsområden som möjligt. Detta medför att it-komponenter generellt är sårbara om anpassningar inte sker. Vanligen krävs förändringar av exempelvis behörigheter, systemparametrar och andra systeminställningar för att komponenten ska optimeras till sin avsedda miljö och funktion. Härdningsprocessen förbättrar generellt säkerheten i it-komponenter, framför allt eftersom sårbarheter minskar.

5.3.2 Instruktioner för hur en it-komponent ska används

Det ska finnas instruktioner som beskriver hur it-komponenten får användas med utgångspunkt från dess skyddsnivå. Användare av it-komponenter ska informeras om hur de ska hantera resursen samt vilka villkor och vilket ansvar som gäller för åtkomst. Instruktionerna kan exempelvis handla om följande:

- Nätverk: Hur ska autentisering av individer ske? Vilket är användningsområdet? Vilka tjänster får användas? Hur ska utrustning som ansluts till nätverk identifieras?
- It-arbetsplatser: Hur ska åtkomst och autentisering ske? Vilka regler gäller för programinstallationer som utförs av användare? Vilka systemparametrar får ändras?

ID	Regler och anvisningar för hantering av tillgångar
I 13.1 0 1 2 3	Samtliga relevanta it-komponenter ska identifieras och förtecknas samt förvaltas löpande.
I 13.2 0 1 2 3	En komplett förteckning över samtliga relevanta it-komponenter ska upprättas och underhållas. Rutiner ska finnas för att hålla förteckningen aktuell och förteckningen ska skyddas från åtkomst eller förändring av obehörig.
I 13.3 0 1 2 3	Om en it-komponent hanterar flera typer av information är det informationen med högst klassning avgör it-komponentens skyddsbehov.
I 13.4 0 1 2 3	It-komponenter ska ha en skyddsnivå som baseras på klassningen av den information som hanteras i it-komponenten eller baserat på andra objekt som it-komponenten stödjer eller påverkar.
I 13.5 0 1 2 3	Skyddsåtgärderna kring en it-komponent ska motsvara skyddsbehovet så att rätt nivå av säkerhet upprätthålls under it-komponentens hela livscykel, dvs. vid införande, under drift och till dess att den avvecklats.
I 13.6 0 1 2 3	Informationssäkerhetskrav som gäller användning av it-komponenter ska finnas med i användarinstruktioner.
I 13.7 0 1 2 3	En process för utformning av it-tekniska skyddsåtgärder ska finnas och underhållas samt synkroniseras med skyddsnivåer.



Figur 29. Figuren visar en processkarta för skyddsbehovet hos en resurs, analys och införande av tekniska skyddsåtgärder ur det it-nära perspektivet. Processkartan börjar med ruta för “Identifiera resursskyddsbehov utifrån informationstyper. Nästa steg är att identifiera en lämplig skyddsnivå, därefter leds man till rutan “Överensstämmer skyddsbehovet?” Om ja lämnas resursen vidare till förvaltning, sedan vidare till riskägare kommundirektör som kalkylerar kvarstående risk och lämnar till sist vidare resursen till objektägaren, samt informerar om kvarstående risk.

Om skyddsbehovet inte överensstämmer slussas resursen vidare till en annan ruta för att identifiera samt värdera risker, med hjälp av riskanalyser. Här värderas riskerna och utreds sedan för förbättringsmöjligheter. Detta dokumenteras och informationsägare informeras om förändrat skydd, och överlämnas sedan till förvaltning. Viden utredning där lämpligt skydd saknas elle rinte kan införas,

skickas det vidare till informationssäkerhetsrådet som kommer med utlåtande. Därefter gör kommundirektören ett beslut kring ja eller nej.

5.4 Styrning av åtkomst

Styrning av åtkomst är en grundläggande skyddsåtgärd för att skydda information och it-komponenter. Behörighet innebär vissa rättigheter att använda information i exempelvis ett it-system, en molntjänst eller en it-tjänst på ett specificerat sätt. Behörigheterna definierar vad en användare har rätt att göra, t.ex. läsa, söka, skriva, radera, skapa information eller köra ett program.

Behörigheter ska tilldelas baserat på en användares behov till information (s.k. need to know) och till de it-komponenter (molntjänster, system, databaser, operativsystem eller nätverk) som personen behöver för att utföra sina arbetsuppgifter.

Inom it-nära verksamhet [18]kan medarbetare behöva behörighet till en mängd it-komponenter och därigenom få åtkomst till en stor mängd information där det på förhand kan vara svårt att definiera arbetsuppgiften.

I dessa fall kompletteras teknisk behörighetskontroll med regelstyrd åtkomstkontroll. Regler ska finnas som beskriver att medarbetare inte får ta del av information som inte rör dennas arbetsuppgifter. För att tillgodose informationssäkerheten ska det dessutom finnas rutiner för att följa upp användares aktiviteter, exempelvis funktioner för övervakning och loggning, om informationen är klassad som sekretess eller stark sekretess.

Behörighetskontrollsystem (BKS) består av både tekniska system och organisatoriska rutiner. Ett BKS omfattar följande säkerhetsåtgärder:

- identifiering och autentisering av användares uppgivna identitet
- tilldelning av behörigheter till it-komponent
- reglering av åtkomsträttigheter, dvs. vilken information användaren kommer åt och vad denna kan göra med den, t.ex. läsa, skriva, ändra eller radera
- loggning av användarens aktiviteter.

5.4.1 Identifiering och autentisering

Inloggningskonto och lösenord tillsammans är ett sätt att autentisera en användare, dvs. verifiering av en uppgiven identitet (se även kapitel 2.5 – Identifiering, inloggningskonton och behörigheter för utformning av lösenord, regel M5.1 och M5.2). Autentiseringen innebär att aktiviteter och åtkomst till en it-komponent kan knytas till en enskild persons identitet. Därför ska samtliga inloggningskonton vara unika och personliga. Även utgivningsprocessen ska vara säkrad. Stark autentisering [19]innebär identifiering av en person och verifiering av

[18] Observera att it-nära verksamhet även kan gälla enheter i andra organisationer, inte bara LKDATA.
[19] Kallas även tvåfaktorsautentisering. Integritetsskyddsmyndigheten använder begreppet ”säker identifiering”. För ytterligare nivå av säkerhet kan samtliga tre faktorer användas gemensamt, s.k. trefaktorsautentisering.

personens autenticitet genom en kombination av minst två av följande tre faktorer som är unika för personen:

- ett lösenord, en pin-kod eller någonting annat som man vet
- ett smartkort, en nyckel eller någonting annat som man har
- ett fingeravtryck, en ansiktsbild eller någonting annat som man är.

Det ska finnas skyddsåtgärder som säkerställer att lösenord skyddas från exempelvis administratör eller handläggare oavsett om lösenordet tilldelas, förändras eller återställs. Detta gäller interna användare såväl som extern användare.

ID	Regler och anvisningar för identifiering och autentisering
V 14.1 	Alla användare ska ha ett unikt inloggningskonto.
V 14.2 	Namn på användare som underlag för t.ex. e-postadresser ska vara enhetliga i kommunen.
V 14.3 	Vid åtkomst till information med höga skyddsbehov avseende konfidentialitet, riktighet eller spårbarhet ska stark autentisering användas.
V 14.4 	Stark autentisering ska användas vid fjärråtkomst via öppna nät till kommunens it-komponenter.
V 14.5 	Lösenord är alltid information med stark sekretess och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsåtgärder vidtas: ● Tekniska funktioner ska implementeras i it-komponenten där så är möjligt för att säkerställa att lösenordsregler för medarbetare följs. ● Lösenord ska aldrig skickas eller transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. ● Lösenord ska lagras krypterat. Felaktig inmatning av lösenord upprepade gånger ska leda till att inloggningskontot stängs. Händelserna ska loggas.
V 14.6 	Samtliga klienter (datorer samt mobila enheter där det så är möjligt) ska förses med automatiskt skärmlås efter 10 minuters inaktivitet för att minska risken för obehörig åtkomst. Aktivering kan endast ske genom en förnyad autentisering.

Bild: Bilden visar en tumme som scannas för fingeravtryck.

5.4.2 Reglering av behörigheter

Det ska finnas dokumenterade rutiner för behörighetshantering. Detta inkluderar att underhålla och förvalta behörigheter, t.ex. hantera beställning av, ändra och ta bort behörigheter så att användares roller och åtkomst till information återspeglas i behörigheterna.

Rutiner ska kopplas till verksamheterna genom en personalfunktion eller ett ansvar för rollen kontoadministratör, vilket säkerställer att behörigheter regleras när någon anställs, när någons roll eller arbetsuppgifter förändras eller när någons anställning upphör.

It-säkerhetssamordnaren ansvarar för att		Fördjupad information
●	Objektägare it ansvarar för att upprätta ett BKS som motsvarar aktuell it-komponents skyddsbehov och krav på behörighetsstyrning.	Kapitel 5.2 – It-nära roller och ansvar

Informationsägare, informationsägarbiträde eller objektägare verksamhet beslutar vem som ska ha behörighet till respektive verksamhets it-system och it-tjänster. Objektägare it ansvarar för att upprätta ett BKS som motsvarar skyddsprofilen. Objektägare it ansvarar även för att upprätta funktioner som kan redogöra för systemets användare och deras behörigheter.

För externa användare (t.ex. konsulter) gäller signering av blankett för tystnadsplikt och tidsbegränsad behörighet, utöver de regler som gäller all behörighetstilldelning. Tiden för

tilldelning av behörighet ska begränsas till den tid som behövs för att utföra uppgiften eller till den tid som anges i aktuellt avtal.

Utökade behörigheter ska tilldelas restriktivt. En person ska endast ha tillräckliga behörigheter för att kunna utföra sitt uppdrag.

För användare med utökade (administrativa) behörigheter (även kallade. administrativa konton) ska revision av behörigheter ske minst två gånger per år. Det gäller för såväl Active Directory som exempelvis databaser (SA i MS-SQL).

Det ska också finnas rutiner för att gå igenom och revidera en persons behörighet när personen byter tjänst.

ID	Regler och anvisningar för identifiering och autentisering
I 14.7 0 1 2 3	Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering kopplat till it-komponenter med BKS.
I 14.8 0 1 2 3	Inloggningskonton för it-komponenter med BKS, och vilka personer dessa tillhör, ska registreras i en gemensam förteckning. En rutin ska finnas för att hålla denna förteckning uppdaterad. För att garantera spårbarhet ska rutinen även innehålla en kontrollfunktion, så att inte tidigare inloggningskontons benämning (namn) återanvänds för en annan person. Det ska också finnas en historikfunktion, så att förteckningen kan visa vilka inloggningskonton som funnits och vilka personer dessa konton tillhörde vid en given tidpunkt.
I 14.9 0 1 2 3	Behörigheter till relevanta it-komponenter (tjänster och system) ska vara dokumenterade i en förteckning med den åtkomst som beslutats. En rutin ska finnas för att hålla denna förteckning uppdaterad. Det ska även finnas en historikfunktion, så att förteckningen kan visa vilka personer som hade åtkomst till en viss relevant it-komponent vid en given tidpunkt.
I 14.10 0 1 2 3	Behörigheter som inte längre behövs ska inaktiveras skyndsamt. För relevanta it-komponenter gäller att inaktivering av behörighet ska ske inom en arbetsdag.
I 14.11 0 1 2 3	Det ska finnas rutiner kopplade till verksamheternas personalfunktion för att säkerställa att reglering av behörigheter sker vid förändrade roller, förändrade arbetsuppgifter eller när en anställning upphör.
I 14.12 0 1 2 3	Tilldelning av administrativa behörigheter ska ske restriktivt samt vara motiverad och tidsbegränsad. Administrativa konton (inloggningskonton med utökade behörigheter) ska ha ökade krav på komplexa lösenord. Objektägare verksamhet eller objektägare it ansvarar för tilldelning av administrativa behörigheter. Tilldelning av utökade behörigheter till en klientdator (utvecklingsdator) ska ges restriktivt och motiveras.
ID	Regler och anvisningar för identifiering och autentisering

I 14.13 0 1 2 3	Gruppkonton är generellt sett inte tillåtna. Eventuella undantag ska godkännas av både objektägare verksamhet och objektägare it. Undantaget ska noteras i systemets dokumentation. Gruppkonto kan enbart beviljas under följande förutsättningar: • Behovet av gruppkonto är tydligt beskrivet och alternativen utredda så att det framgår varför gruppkontot är nödvändigt. • Gruppkontot har en registrerad ägare. • Gruppkontot är tidsbegränsat med tydligt slutdatum. • Endast information som samtliga i gruppen har behörighet att läsa, redigera och lagra får hanteras. • Ägaren av gruppkontot ska göra en förteckning över alla som använder kontot. Historikfunktion ska finnas så att man i efterhand kan visa vilka användare som haft tillgång till kontot vid en given tidpunkt. • Autentiseringsinformation ska uppdateras och distribueras på nytt om någon användare inte längre har behörighet till gruppkontot. • Ägaren av ett gruppkonto har tillsynsansvar för eventuellt missbruk av gruppkontot.
I 14.14 0 1 2 3	Inloggningskonton knutna till externa användare ska kunna särskiljas från inloggningskonton knutna till interna användare. För externa användare gäller utöver övriga regler för behörighetstilldelning att tilldelning av behörigheter ska • tidsbegränsas till att endast omfatta den tid som krävs för att utföra uppgiften • föregås av en signering av blankett för tystnadsplikt.
I 14.15 3	En individuell prövning ska ha skett och blankett för tystnadsplikt ska vara signerad innan åtkomst tilldelas till för en it-komponent som innehåller information med stark sekretess.
I 14.16 0 1 2 3	Relevanta it-komponenter ska där så är möjligt ha BKS som motsvarar deras skyddsnivå.

5.5 Kryptering

Kryptering kan användas för flera ändamål, t.ex. för att förhindra att någon obehörig får åtkomst till information, och kryptografiska signaturer kan garantera informationens integritet eller äkthet.

Ansvar för kryptering		Fördjupad information
●	It-säkerhetssamordnaren ansvarar för att tillhandahålla krypteringslösningar baserade på it-komponenters skyddsnivå.	Kapitel 5.2 – It-nära roller och ansvar

LKDATA ska vid behov tillhandahålla godkända krypteringslösningar och instruktioner om hur dessa ska användas. Behov av kryptering ska baseras på skyddsbehovet. Kryptering ska alltid användas om det föreligger höga skyddsbehov på konfidentialitet eller riktighet.

Krypteringslösningarna ska bygga på etablerade standarder. Lösningarna ska föreslås, granskas och godkänns av it-säkerhetssamordnaren i samråd med informationssäkerhetsrådet.

Krypteringslösningar bygger ofta på certifikat. Säkerheten för dem hanteras genom återkallande (revokering) och validering.

- revokering av certifikat gör det möjligt att avsluta åtkomst till it-komponenter
- validering gör det möjligt att dels avgöra om ett certifikat är giltigt, dels
- kontrollera innehavaren

I system som använder kryptonycklar kan dessa säkerhetskopieras. Här ställs stora krav på åtkomstkontroll, organisatoriska rutiner och loggning, så att -åtkomsten till nycklar kan spåras.

ID	Regler och anvisningar för kryptering
I 5.1 	Krypteringslösningar ska baseras på etablerade standarder. Dessa lösningar ska godkännas av informationssäkerhetsrådet.
I 5.2 	nloggningskonton för it-komponenter med BKS, och vilka personer dessa tillhör, ska registreras i en gemensam förteckning. En rutin ska Certifikathantering ska säkerställas för att tillgodose de krav som finns för it-komponent vad gäller revokering av certifikat validering av certifikats giltighet och autenticitet för att hålla denna förteckning uppdaterad. För att garantera spårbarhet ska rutinen även innehålla en kontrollfunktion, så att inte tidigare inloggningskontons benämning (namn) återanvänds för en annan person. Det ska också finnas en historikfunktion, så att förteckningen kan visa vilka inloggningskonton som funnits och vilka personer dessa konton tillhörde vid en given tidpunkt.
I 5.3 	Krypteringsnycklar är information med stark sekretess och ska skyddas.
I 5.4 	Kryptering av information i olika it-komponenter ska baseras på it-komponenters skyddsprofil.

5.6 Fysisk säkerhet för it-komponenter

Fysisk och miljörelaterad säkerhet handlar om att förhindra otillåten fysisk åtkomst till, skador på och störningar i it-komponenter och den information som komponenten hanterar. (Skyddsåtgärder och krav på fysisk och miljörelaterad säkerhet beskrivs i kapitel 6 – Informationssäkerhet och fysiskt skydd.)

5.7 It-driftsäkerhet

Driftsrutiner

Driftsrutiner ska finnas för relevanta it-komponenter gällande

- installation och konfiguration
- uppstart och nedtagning
- säkerhetskopiering (t.ex. RPO- och RTO-krav)
- underhåll av utrustning
- supportkontakter vid oväntade funktionella eller tekniska problem
- hantering av media
- loggning
- övervakning.

Ansvar för driftsrutiner		Fördjupad information
●	Objektägare it ansvarar för driften av samtliga it-komponenter som ingår i objektkatalogen. För it-komponenter som driftas av LKDATA men inte ingår som ett förvaltningsobjekt ansvarar CIO.	Kapitel 5.2 – It-nära roller och ansvar

Det ska finnas rutiner för att hantera ändringar i driftsmiljön (driftssäkerhet). För att minska risken för obehörig åtkomst ska även driftsmiljön ska vara separerad från test- och utvecklingsmiljön.

ID	Regler och anvisningar för kryptering
I 7.1 0 1 2 3	Det ska finnas beslutade och dokumenterade driftsrutiner för relevanta it-komponenter (processer och objekt). Dessa ska göras tillgängliga för alla administratörer som behöver dem.
I 7.2 0 1 2 3	Ändringar i it-komponenter ska följa fastställda processer som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända (s.k. change management).
I 7.3 0 1 2 3	Utvecklings-, test- och driftsmiljöer ska vara separerade. Graden av separation ska utföras till den nivå som bedöms lämplig och möjlig.

5.7.1 Skydd mot skadlig kod

När det gäller skadlig kod ska det finnas metoder för att dels förebygga och upptäcka skadlig kod, dels återställa it-komponenter efter angrepp.

Ansvar för skydd mot skadlig kod		Fördjupad information
●	It-säkerhetssamordnaren ansvarar för att tillhandahålla lösningar för skydd mot skadlig kod baserade på skyddsnivå.	Kapitel 5.2 – It-nära roller och ansvar

Kommunens relevanta it-komponenter, framför allt servrar och klienter, ska skyddas från skadlig kod genom att endast godkänd programvara installeras eller körs. Skyddet ska regelbundet uppdateras enligt tillverkarens rekommendationer.

Programvara ska i förebyggande syfte söka efter skadlig kod i

- datorer i kommunens nätverk
- e-post
- information som överförs via nätverk.

Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för att återställa it-komponenter (se kapitel 5.11 – Incidenthantering).

Det ska finnas en process för att säkerställa att säkerhetsuppdateringar genomförs för att hålla system och applikationer fria från säkerhetsbrister som kan utnyttjas av skadlig kod. Det ska även finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. genom prenumeration på nyhetstjänster och bevakning av webbplatser som ger information om ny skadlig kod (t.ex. www.cert.se).

ID	Regler och anvisningar för skadlig kod
I 7.4 0 1 2 3	Det ska finnas metoder och programvara som förebygger och upptäcker skadlig kod (programvara) samt återställer kommunens it-miljö efter angrepp (metod). Alla relevanta it-komponenter, framför allt servrar och klienter, ska ha ett skydd mot skadlig kod. Skyddet ska installeras och underhållas enligt tillverkarens rekommendationer.
I 7.5 0 1 2 3	System och applikationer ska regelbundet uppdateras för att hållas fria från säkerhetsbrister och risken att utsättas för skadlig kod.
I 7.6 0 1 2 3	Det ska finnas en fastställd rutin för att återställa relevanta it--komponenter om kommunen skulle drabbas av skadlig kod som -orsakar driftavbrott (virusutbrott).
I 7.7 0 1 2 3	Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. genom prenumeration på nyhetstjänster eller bevakning av webbplatser som ger information om ny skadlig kod (t.ex. www.cert.se).

5.7.2 Säkerhetskopiering

Säkerhetskopiering är en skyddsåtgärd för tillgänglighet, riktighet och spårbarhet, och behovet ska kopplas till informationsklassningen. Om klassningen visar att det finns höga skyddsbehov för tillgänglighet ska vanligen redundans säkerställas i de it-komponenter (system, lagring, nät-verk) som behövs för att leverera tjänsten. Vid lägre klassning är det normalt tillräckligt att använda säkerhetskopior och återställningsrutiner.

Korttidslagrade säkerhetskopior ska skyddas i säkert utrymme avsett för datamedia. Långtidslagrade säkerhetskopior ska förvaras geografiskt åtskilda från originalmaterialet för att minska risken att all information går förlorad vid exempelvis brand (se även kapitel 6 – Informationssäkerhet och fysiskt skydd).

Säkerhetskopior ska testas regelbundet för att säkerställa att informationen kan återställas. Flera generationer av säkerhetskopior ska utformas så att verksamheter undviker att förlora långtidslagrad information.

ID	Regler och anvisningar för säkerhetskopiering
I 7.8 0 1 2 3	För it-komponenter med höga skyddsbehov vad gäller tillgänglighet (höga RPO-krav) ska det finnas redundans i delkomponenter, system, lagring och nätverk. Tillgänglighet ska övervakas med automatiska larm som larmar om viktiga kvalitetsmått inte uppfylls. Gränsvärden för larm ska sättas så att målet för återställningstid säkerställs. Automatiska larm ska testas regelbundet.
I 7.9 0 1 2 3	Krav ska definieras för säkerhetskopiering av information baserat på objekts klassning av riktighet, tillgänglighet och spårbarhet. Dessa krav ska minst reglera vilken information som ska omfattas av säkerhetskopiering, hur lång tid säkerhetskopior ska sparas innan gallring samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar. Maximal informationsförlust och mål för återställningstid ska definieras för varje it-komponent och tillsammans med övriga krav ligga till grund för vald lösning för säkerhetskopiering.
I 7.10 0 1 2 3	Det ska finnas en process för att återställa information från säkerhetskopior. Processen ska vara testad och dokumenterad för respektive it-komponent.
I 7.11 3	Säkerhetskopiering av it-komponenter med höga skyddsbehov vad gäller tillgänglighet (höga RTO-krav) ska lagras på lämplig media för att skyndsamt kunna återställas. Övervakning av funktionen ska konfigureras med automatlarm.
I 7.12 0 1 2 3	Säkerhetskopior av information ska hanteras med samma skyddskrav för konfidentialitet som de system som lagrade originalinformationen.
I 7.13 0 1 2 3	Säkerhetskopior som korttidslagras ska skyddas genom ett säkert utrymme avsett för datamedia.
I 7.14 0 1 2 3	Säkerhetskopior för långtidslagring ska lagras geografiskt åtskilda från originalmaterialet.
I 7.15 0 1 2 3	Generationer av säkerhetskopior ska vara möjliga att utforma så att verksamheter undviker att förlora långtidslagrad information.

5.7.3 Loggning

Loggning av händelser utgör grunden för god spårbarhet i it-komponenter. Även konfidentialitet, riktighet och tillgänglighet är till stor del beroende av bra logghantering.

It-komponenters skyddsnivå utgör grunden för behovet av loggar, och it-komponentens art och användningsområde avgör vilka loggar som är relevanta. Överväg t.ex. följande loggar för it-komponenter:

- inloggningskonto med datum, tider och uppgifter om inloggning och utloggning
- it-komponentens identitet eller plats (om möjligt) samt systemidentifierare lyckade och misslyckade åtkomstförsök

Överväg t.ex. följande loggar för information som hanteras med förhöjda skyddsbehov:

- förändringar i systemkonfiguration
- nätverksadresser och portar
- aktivering och inaktivering av säkerhetsverktyg, t.ex. antivirussystem och system för att upptäcka och stoppa intrång
- användaraktiviteter i tillämpningar (med förhöjda skyddsbehov).

Överväg t.ex. följande loggar för information som hanteras med höga skyddsbehov:

- poster av lyckade och misslyckade åtkomstförsök till data och andra resurser med höga skyddsbehov gällande konfidentialitet, riktighet och spårbarhet
- användning av administrativa behörigheter
- användning av systemverktyg och tillämpningar
- åtkomst till filer och typ av åtkomst.

Händelser i olika it-komponenter kan korreleras genom loggverktyg och genom att alla loggkällor använder gemensam och korrekt tid, vilket ger en mer heltäckande bild av händelser jämfört med om en logg övervakas i varje komponent för sig. Observera att loggning kan styras utifrån gällande lagstiftning.

ID	Regler och anvisningar för säkerhetskopiering
I 7.16 0 1 2 3	Loggning av olika händelser ska ske i it-komponenter. Typ och omfattning av loggar ska bl.a. baseras på it-komponenternas skyddsnivå.
I 7.17 0 1 2 3	Loggar ska sparas enligt gallringsbeslut (redovisad i IHP:n) samt analyseras och granskas regelbundet av utsedda loggadministratörer.
I 7.18 0 1 2 3	Systemklockorna i alla relevanta it-komponenter ska synkroniseras mot en referenskälla för korrekt tid.
I 7.19 0 1 2 3	Logginformation ska skyddas mot manipulation och obehörig åtkomst på samma nivåer för spårbarhet och konfidentialitet som det system loggen genereras ifrån.
I 7.20 0 1 2 3	Loggning kan styras utifrån gällande lagstiftning och ska minst utformas så att denna upprätthålls.

5.7.4 Övervakning

Övervakning av it-komponenter är basen för god tillgänglighet. Den tjänst och de resurser som används för övervakning ska alltid hanteras som skyddsvärd eftersom driftstörningar kan medföra svårigheter att analysera orsaker till incidenter.

Ansvar för skydd mot skadlig kod		Fördjupad information
●	Objektägare it ansvarar för övervakning av it-komponenter som ingår i förvaltningsobjekten. För it-komponenter som driftas av LKDATA men inte ingår som ett förvaltningsobjekt ansvarar CIO för relevant övervakning.	Kapitel 5.2 – It-nära roller och ansvar

Den beslutade skyddsnivån utgör grunden för behovet av övervakning av it-komponenter. Den avgör även hur övervakningen ska ske. Egenskaper, händelser eller situationer som bör övervägas för övervakning för it-komponenter är

- nod/tjänst aktiv
- gränsvärden och trender
- aktivt larmande noder (t.ex. SNMP-traps)
- säkerhetsegenskaper i använda övervakningsprotokoll
- placering och säkerhet för övervakande resurs.

ID	Regler och anvisningar för övervakning
I 7.21 0 1 2 3	Loggning av olika händelser ska ske i it-komponenter. Typ och omfattning av loggar ska bl.a. baseras på it-komponenternas skyddsnivå.

5.7.5 Speciella it-system

Vissa typer av system baseras inte på PC-datorer och motsvarande. Sådana system återfinns framför allt inom produktion av el, värme eller vatten men även inom transportsektorn. System för fastighetsautomation, t.ex. styrning av ventilation, värme och belysning, är andra exempel på system som numera moderniseras och ansluts med ny teknik och integreras på nya sätt.

Ansvar för speciella it-system		Fördjupad information
●	Objektägare it ansvarar för speciella system som ingår i förvaltningsobjekten. För speciella system som driftas av LKDATA men inte ingår som ett förvaltningsobjekt ansvarar CIO.	Kapitel 5.2 – It-nära roller och ansvar

Gemensamt för dessa system är att de styr någon fysisk process eller olika fysiska enheter, och de brukar kallas industrial control systems (ICS), vilket översätts med industriella kontroll- och styrsystem, inbäddade system eller it-baserade styrsystem. Utvecklingen och digitaliseringen har medfört att dessa system allt mer bygger på samma teknik som administrativa it-system och de drabbas därmed av samma sårbarheter.

Eftersom konsekvenserna av en incident i dessa system är annorlunda än vid -incidenter i administrativa system krävs det att verksamheter hanterar kravbilden på andra sätt. Var därför noggrann med att kartlägga dessa typer av system och utför separata riskanalyser om så krävs.

ID	Regler och anvisningar för speciella it-system

I 7.22 0 1 2 3	För industriella kontroll- och styrsystem kan riskbilden vara förändrad. Var därför noggrann med att kartlägga dessa typer av system och utför riskanalyser om så krävs.

5.7.6 Hantering av tekniska sårbarheter

Tekniska sårbarheter i it-komponenter kan innebära att komponenter exponeras för skadlig kod, dataintrång eller andra sårbarheter. Därför ska det finnas rutiner så att information om tekniska sårbarheter fås i tid och att sårbarheter analyseras så att lämpliga åtgärder kan vidtas.

Ansvar för hantering av tekniska sårbarheter		Fördjupad information
●	Objektägare it ansvarar för att information om tekniska sårbarheter fås i tid och att lämpliga åtgärder vidtas för it-komponenter som ingår i förvaltningsobjekten. För övriga it-komponenter som driftas eller som ansvaras av LKDATA men som inte ingår som ett förvaltningsobjekt ansvarar CIO.	Kapitel 5.2 – It-nära roller och ansvar

Okontrollerad installation av program kan medföra sårbarheter, exempelvis obehörig åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter. Regler och anvisningar för programinstallationer ska därför upprättas och införas för att definiera vilka typer av program som kan installeras och på vilket sätt.

ID	Regler och anvisningar för hantering av tekniska sårbarheter
I 7.23 0 1 2 3	Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i it-komponenter. Uppdateringar och säkerhetsuppdateringar ska göras regelbundet av it-komponenter.
I 7.24 0 1 2 3	Om säkerhetsuppdatering inte är praktiskt möjlig ska information om tekniska sårbarheter i dessa it-komponenter inhämtas och analyseras samt lämpliga åtgärder vidtas för att hantera eventuella risker.
I 7.25 0 1 2 3	Säkerhetsgranskning av it-komponenter som exponeras mot internet ska ske regelbundet och vid nyanskaffning, för att kontrollera dels att inga uppenbara sårbarheter exponeras, dels att tillräcklig skyddsnivå upprätthålls. Sådan granskning kan t.ex. bestå av skanning av sårbarheter med automatiserade verktyg eller s.k. penetrationstester.
I 7.26	Det ska finnas anvisningar för samtliga plattformar och program-

0 1 2 3	installationer. Dessa anvisningar ska definiera på vilket sätt installationer ska utföras.

5.8 Kommunikationssäkerhet

Kommunikationssäkerhet innebär ett skydd i de it-komponenter och nätverk som används för datakommunikation. Syftet är att skydda den information som kommuniceras, vilket är viktigt framför allt ur ett riktighetsperspektiv.

Ansvar för kommunikationssäkerhet		Fördjupad information
●	Objektägare it ansvarar för kommunikationssäkerhet för it-komponenter som ingår i förvalt-ningsobjekten. För kommunikationssäkerhet för övriga it-komponenter som driftas eller som ansvaras av LKDATA men som inte ingår som ett förvaltningsobjekt ansvarar CIO.	Kapitel 5.2 – It-nära roller och ansvar

5.8.1 Nätverkssäkerhet

Nätverk ska hanteras och styras för att skydda information i anslutna system och tillämpningar. Rutiner ska finnas för hur nätverk förvaltas av ansvariga ägare till nätverk.

Anslutna it-komponenters skyddsnivå är grunden för vilka skyddsåtgärder som ska finnas för att nå säkerhet för informationen i ett nätverk. Krav på skyddsåtgärder ska inkluderas i avtal för nätverkstjänster som tillhandahålls av extern part. Skyddsåtgärder för nätverkssäkerhet kan exempelvis vara:

- autentisering av system
- kryptering
- regler för säkerhet och nätverksanslutning
- begränsning av systemanslutningar
- brandväggar och intrångsdetekteringssystem
- loggning och övervakning av nätverk
- separation av nätverk (segmentering).

En grundläggande segmentering av ett nätverk innebär att man dels skiljer interna nät från internet, dels skiljer det interna nätet mellan olika verksamheter och avdelningar från varandra. Men kan även vid behov skilja utvecklings-, test- och produktionsmiljöer från varandra. Brandväggsregler i nätverk behöver vidimeras regelbundet för att hållas uppdaterade med rätt regler för kommunikation mellan de olika nätsegmenten.

ID	Regler och anvisningar för nätverkssäkerhet
I 8.1 0 1 2 3	Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverks-tjänster om dessa tjänster tillhandahålls av extern part.
I 8.2 0 1 2 3	Teknik för att kryptera och säkra trådlös datakommunikation ska alltid användas, oavsett skyddsbehov.
I 8.3 2 3	Trådlös datakommunikation som innehåller information med förhöjda eller höga skyddsbehov vad gäller konfidentialitet är endast tillåten från godkända klienter.
I 8.4 0 1 2 3	En segmentering av nätverket ska göras för att skilja interna nät från internet, för att skilja olika verksamheter från varandra samt för att vid behov skilja test-, utvecklings- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan segmenteras ytterligare i separata nätverk, utifrån skyddsbehov.
I 8.5 0 1 2 3	Utrustning och metoder ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.
I 8.6 0 1 2 3	Dokumentation ska upprättas för kommunikation mellan olika segment. Dokumentationen ska innehålla information om syfte, skyddsnivå och skyddsbehov.
I 8.7 0 1 2 3	Brandväggar ska konfigureras enligt dokumenterade regler. Av reglerna ska det framgå vilka nätverkstjänster som ska tillåtas samt vilka händelser och aktiviteter som ska loggas och följas upp. Brandväggar och dess regler ska revideras regelbundet.
I 8.8 0 1 2 3	Kommunikationstjänster mellan Linköpings kommun och externa nätverk ska dokumenteras och godkännas av objektägare it innan inkoppling får ske.

5.8.2 Informationsöverföring mellan it-system

Överföring av information från ett system till ett annat får endast ske om det mottagande systemet uppfyller minst det skyddsbehov som den överförda informationen kräver. Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Lösningar med kryptering och om möjligt signering ska användas om information med förhöjda eller höga skyddsbehov ska överföras.

Avtal som reglerar säker överföring av verksamhetsinformation mellan kommunen och extern part ska upprättas. Användandet av osäkra metoder får inte nyttjas om information

ska överföras med förhöjda eller höga skyddsbehov vad gäller konfidentialitet.

ID	Regler och anvisningar för nätverkssäkerhet
I 8.9 	Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverks-tjänster om dessa tjänster tillhandahålls av extern part.
I 8.10 	Teknik för att kryptera och säkra trådlös datakommunikation ska alltid användas, oavsett skyddsbehov.
I 8.11 	Trådlös datakommunikation som innehåller information med förhöjda eller höga skyddsbehov vad gäller konfidentialitet är endast tillåten från godkända klienter.
I 8.12 	En segmentering av nätverket ska göras för att skilja interna nät från internet, för att skilja olika verksamheter från varandra samt för att vid behov skilja test-, utvecklings- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan segmenteras ytterligare i separata nätverk, utifrån skyddsbehov.
I 8.13 	Utrustning och metoder ska finnas för att kontrollera och förhindra obehörig nätverkstrafik mellan olika nätverkssegment.

5.9 Anskaffning och utveckling av it-komponenter

Relevant informationssäkerhet för it-komponenter ska säkerställas för en it-komponents hela livscykel – från anskaffning eller utveckling till utrangering eller kassering.

Ansvar för anskaffning och utveckling		Fördjupad information
●	Objektägare it ansvarar för att informationssäkerhetskrav finns tillgodosedda vid anskaffning och utveckling av it-komponenter som ingår i förvaltningsobjekten. För övriga it-komponenter som utvecklas eller anskaffas av LKDATA ansvarar CIO.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.2 – It-nära roller och ansvar

5.9.1 Informationssäkerhetskrav på it-komponenter

De behov som rör informationssäkerhet ska inkluderas både som krav för nya it-komponenter och när befintliga komponenter förbättras. Det gäller oavsett om it-komponenten anskaffas externt, utvecklas internt eller kombinerar båda, t.ex. vid intern anpassning av ett externt köpt standardsystem.

Informationssäkerhetskraven ska spegla den skyddsnivå som tilldelats it-komponenten, vilken baseras på skyddsbehovet (informationsklassningen) samt eventuella kompletterande riskanalyser.

Förvaltningsorganisationen ska involveras när it-komponenter i form av tjänster och system som omfattas av verksamhetsnära förvaltning utvecklas, anskaffas eller förändras. Objektägare it ansvarar för att tekniska informationssäkerhetskrav formuleras och dokumenteras på ett sätt som överensstämmer med verksamhetens behov, så att it-komponenten får ett skydd som korrelerar med den information komponenten hanterar.

Innan it-komponenten anskaffas, utvecklas eller förändras ska dessa krav granskas av de parter som har ett intresse av att den information som hanteras i it-komponenten får ett relevant skydd.När underliggande it-komponenter i form av infrastruktur, stödsystem m.m. utvecklas, anskaffas eller förändras ska dessa omfattas av minst samma skyddsnivå som de it-komponenter de stöder. Ibland kan kraven dessutom vara högre, exempelvis om en it-komponent stödjer ett stort antal icke-kritiskait-komponenter som tillsammans är kritiska.

ID	Regler och anvisningar för informationssäkerhetskrav på it-komponenter
I 9.1 0 1 2 3	Behoven av informationssäkerhet ska inkluderas som krav för nya it-komponenter samt när befintliga it-komponenter förändras.
I 9.2 0 1 2 3	Informationssäkerhetskraven ska baseras på den skyddsprofil som tilldelats it-komponenten. Informationssäkerhetskraven ska dokumenteras och granskas av berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.
I 9.3 0 1 2 3	Varje it-komponents säkerhetsdesign ska dokumenteras. Dokumentationen ska visa hur skyddsbehovet för informationen som hanteras i it-komponenten säkerställs.

5.9.2 Informationssäkerhet vid systemutveckling

När it-komponenter utvecklas ska processer, rutiner och etablerade modeller för utveckling av säker programvara finnas på plats för att säkerställa informationssäkerheten. Säkerhet ska vara en integrerad del av utvecklingsprocessen.

Vid systemutveckling och integration ska utvecklingsmiljöer upprättas och skyddas över it-komponentens hela livscykel. En säker utvecklingsmiljö inkluderar de människor, de processer och den teknik som är involverade i systemutveckling och integration. Det innebär att alla utvecklare måste ha kompetens i säker programutveckling.

Beställd systemutveckling från extern part ska styras och övervakas, och säkerhetsfunktionalitet ska säkerställas. Leverantören ska använda en etablerad modell för utveckling av säker programvara. Om en sådan modell saknas krävs en ingående analys för att säkerställa att leverantören använder en säker utvecklingsprocess.

ID	Regler och anvisningar för it-komponenters livscykel
I 9.4 0 1 2 3	Det ska finnas processer, rutiner och regler som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av it-komponenter.
I 9.5 0 1 2 3	Systemförändringar inom utvecklingscykeln ska styras genom användning av change management-processen.
I 9.6 0 1 2 3	För systemutveckling och integration ska utvecklingsmiljöer upprättas och skyddas över it-komponentens hela livscykel.
I 9.7 0 1 2 3	Systemutvecklare ska ha kompetens i programvarusäkerhet.
I 9.8 0 1 2 3	Vid systemutveckling hos extern part ska krav ställas på en säker utvecklingsprocess.
I 9.9 0 1 2 3	Vid systemutveckling som innehåller personuppgifter ska privacy by design och privacy by default följas.

5.9.3 Informationssäkerhet vid test, utveckling och utbildning

Vid utveckling av it-komponenter ska säkerhetsfunktionaliteten testas gentemot ställda säkerhetskrav och enligt regler och anvisningar för säker utveckling. Vid test kan automatiserade verktyg nyttjas, t.ex. verktyg för kodgranskning eller skanning av sårbarheter. Test bör ske i en realistisk testmiljö för att säkerställa dels att systemet inte för in sårbarheter i organisationens miljö, dels att testerna är tillförlitliga.

Testdata bör skyddas och kontrolleras. System- och acceptanstest kräver normalt sett stora mängder testdata som är så snarlika produktionsdata som möjligt. Att använda produktionsdatabaser för test bör däremot undvikas; om detta inte är möjligt ska personuppgifter i så fall först anonymiseras.

Test-, utvecklings- och driftsmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön. Utvecklare ska inte tillåtas att testa icke fastställda eller icke godkända programversioner i drifts-miljö. Driftsättning ska ske enligt fastställda processer.

ID	Regler och anvisningar för informationssäkerhet vid test, utveckling och utbildning
I 9.10 0 1 2 3	Säkerhetsfunktionalitet ska testas vid utveckling. Test, utveckling och utbildning ska göras gentemot ställda säkerhetskrav och enligt fastställda regler och anvisningar för säker utveckling.
I 9.11 0 1 2 3	Produktionsdata ska i möjligaste mån undvikas om de innehåller förhöjda eller höga skyddsbehov. Om produktionsdata ändå används gäller att ● testdata alltid ska anonymiseras från personuppgifter ● de rutiner för styrning av åtkomst som tillämpas för produktionssystem även ska gälla vid test av produktionssystem ● behörighet ska godkännas av informationsägare, informations-ägarbiträde eller objektägare it ● produktionsdata skyndsamt ska raderas från testsystem efter avslutat test ● kopiering av produktionsdata ska loggas för att uppnå spårbarhet.
I 9.12 0 1 2 3	Utvecklingsversioner får inte placeras i produktionsmiljö. Utvecklings- och driftsmiljöer ska vara separerade på lämpligt sätt för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.
I 9.13 0 1 2 3	Driftsättning ska ske enligt fastställda processer.

5.10 Informationssäkerhetskrav vid upphandling

När it-komponenter ska hanteras eller driftas av underleverantör i form av t.ex. molntjänster ansvarar objektägare it för att leverantören uppfyller samma skyddskrav som om komponenten hanterades internt.

Ansvar vid upphandling		Fördjupad information
●	Vid upphandling är det ansvarig för upphandlingen som ansvarar för att informationssäkerhetskrav är tillgodosedda. Objektägare it ansvarar dock för att informationssäkerhetskrav finns tillgodosedda vid upphandling av it-komponenter som ingår i förvaltningsobjekten. För övriga it-komponenter som upphandlas av LKDATA ansvarar CIO.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 5.2 – It-nära roller och ansvar

Vid en upphandling är det viktigt att vara tydlig i kravställningen, eftersom leverantören kanske använder andra termer eller har en annan uppfattning om vad informationssäkerhet innebär än den som gäller internt i kommunen. Exempelvis är leverantören kanske inte bekant med begrepp som skyddsbehov, klassning av information och it-komponenter, och även om termerna är kända eller bekanta kanske leverantören tillämpar andra nivåer eller tolkar nivåerna på annat sätt.

Det ska säkerställas att leverantörens egen it-miljö uppfyller de skyddsbehov som informationen kräver och har fastställts via informationsklassning och riskanalys. Det ska också säkerställas att leverantörens egna rutiner och personal uppfyller aktuella skyddsbehov.

Avtalet med en extern leverantör ska reglera ansvar för funktionalitet, implemen-tering och upprätthållande av säkerhetsfunktioner samt ansvar för test och verifiering av dessa. Dessutom ska avtalet reglera ansvar för brister som upptäcks över tid. Även personuppgiftsansvar måste beaktas och regleras, vilket även kan påverka kravställningen i upphandlingen.

Se också MSB:s dokument Vägledning för informationssäkerhet vid upphandling.

ID	Regler och anvisningar för informationssäkerhetskrav vid upphandling av it-komponenter
I 10.1 0 1 2 3	Tydliga informationssäkerhetskrav ska ställas vid upphandling av it-komponenter. Kraven ska sedan användas vid utvärdering av anbud och baseras på den skyddsnivå som it-komponenten bedöms tilldelas.
I 10.2 0 1 2 3	Avtal med en leverantör ska alltid redovisa hur leverantören bedriver sitt säkerhetsarbete i sin verksamhet.
I 10.3 0 1 2 3	Avtal med en leverantör ska innefatta stöd och support i händelse av fel och incidenter.
I 10.4 0 1 2 3	Avtal med en leverantör ska reglera hur avtalets uppfyllande kontrolleras, t.ex. genom tredjepartsrevision eller av kommunens egen granskning.
I 10.5 0 1 2 3	Upphandling av it-komponenter som ska vara i drift hos extern leverantör medför ytterligare krav, bl.a. ● fördjupade krav på leverantörens interna it-miljö och informationssäkerhet, t.ex. certifieringar ● leverantörens kontinuitetshantering ● rätt till tredjepartsrevision ● konfidentialitetsavtal ● personuppgiftsbiträdesavtal ● rätt till incidentrapporter från leverantören.
I 10.6 0 1 2 3	Upphandling av it-komponenter ska göras av objektägare it i samverkan med objektägare verksamhet.
I 10.7 0 1 2 3	Avtal med en leverantör ska vid behov innefatta att ● leverantören genomför eller har genomfört säkerhetstestning, säkerhetscertifiering eller motsvarande av it-komponenter före leverans till Linköpings kommun ● kommunen får genomföra tester före leverans ● leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest eller leveranskontroll.
I 10.8 0 1 2 3	Om en leverantör använder underleverantör för hela eller del av leveransen ska ett avtal tecknas som reglerar såväl affärsmässighet som informationssäkerhet mellan leverantör och underleverantör. I ett sådant avtal ska följande punkter beaktas där det är relevant: ● hur applicerbara krav i avtalet med leverantören säkerställs mot underleverantör ● hur rättsliga krav uppfylls, exempelvis lagstiftning om sekretess och personuppgifter ● vilka åtgärder som vidtas för att säkerställa att berörda parter är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, eventuell äganderätt till kod och upphovsrätt ● vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör.

5.11 Incidenthantering

Med en informationssäkerhetsincident avses en händelse med negativ påverkan på en viss informations konfidentialitet, riktighet, tillgänglighet eller spårbarhet. Processer och rutiner ska finnas på plats för att säkerställa en konsekvent och effektiv hantering av informationssäkerhetsincidenter, inklusive kommunikation i samband med incidenterna.

Ansvar för incidenthantering		Fördjupad information
●	Objektägare verksamhet och informationsägare ansvarar för att incidenter hanteras, sammanställs, dokumenteras och förmedlas till informationssäkerhetssamordnaren.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 4.12 – Incidenthantering

För it-nära verksamhet ska fastställda processer användas för att registrera samtliga typer av incidenter. Incidenterna ska märkas så att det i efterhand är enkelt att ta fram historik över dessa. Säkerhetsincidenter ska även rapporteras enligt vad som beskrivs i kapitel 4.12. Den it-nära verksamheten ska alltid medverka och vara stödjande vid utredningar som drivs inom andra verksamheter.Vid incidenter av sådan dignitet att den påverkar kommunens förmåga att bedriva verksamhet eller innebär allvarliga konfidentialitetsbrister ska den it-nära verksamheten omedelbart informera Tjänsteman i beredskap hos -Säkerhetsenheten.

Exempel på informationssäkerhetsincidenter kan vara att
större störningar påverkar tillgänglighet

- obehöriga har fått tillträde till kommunens it-utrymmen
- obehöriga har kommit åt information i ett it-system
- information har ändrats felaktigt eller utan behörighet
- det har skett infektion av virus eller annan skadlig kod
- information som borde ha funnits säkerhetskopierad saknas
- it-komponenter har missbrukats av medarbetare eller externa personer.

En särskilt utsedd person (exempelvis information security manager) leder hanteringen av incidenter i samverkan med berörda objektägare. Vid incidenter relaterade till förvaltningsobjekt ska denna person samverka med relevanta roller i förvaltningsorganisationen.

Vid incidenter eller misstanke om brott ska samverkan ske med chef för berörd verksamhet, säkerhetsenheten, HR-enheten samt juridikenheten. Polisanmälan och insamling av bevis m.m. ska ske i samråd mellan ovan nämnda parter. Var uppmärksam på att att andra typer av incidenter, exempelvis personuppgiftsincidenter, även kan kräva en annan hantering.

Kunskap baserad på analys av hanterade incidenter ska användas för att minska sannolikheten för eller konsekvenser av liknande incidenter i framtiden. Det är viktigt att analysera och lära av incidenter i en process (problem management) för att kunna vidta

åtgärder och förhindra en upprepning av incidenten. Vissa åtgärder kan behöva vidtas skyndsamt och i samband med att en incident inträffar.

Större incidenter (major incidents) sammanställs i incidentrapporter som objektägare it ansvarar för att ta fram i samverkan med incident manager. Mindre incidenter registreras och sammanställs så att informationen sedan kan användas för t.ex. kvantifiering och statistik.

Erfarenheter från inträffade incidenter genom t.ex. incidentrapporter och statistik kan ligga till grund för framtida beslut för att förbättra skyddet, t.ex. om att investera i nya säkerhetslösningar.

ID	Regler och anvisningar för incidenthantering
I 11.1 0 1 2 3	Det ska finnas en process för incidenthantering inom it som omfattar informationssäkerhetsincidenter. Processen ska innefatta ● mottagning av information om incidenten ● styrning av eventuella behov av omedelbara åtgärder, vilka kan vara tillfälliga tills en permanent lösning är på plats ● analys av orsaker till incidenten så att korrigerande och förebyggande åtgärder kan vidtas ● återkoppling till och kommunikation med dem som påverkas av eller är involverade i återhämtning efter incidenten, liksom till den som rapporterat incidenten.
I 11.2 0 1 2 3	Större incidenter (major incidents) ska sammanställas i incident-rapporter där objektägare it deltar i samverkan med incident manager.
I 11.3 0 1 2 3	Inträffade incidenter ska analyseras och kan ligga till grund för beslut om förbättrat skydd.
I 11.4 0 1 2 3	Medarbetare är skyldiga att rapportera såväl informations-säkerhetsincidenter som informations- och it-relaterade brister i system eller tjänster.
I 11.5 0 1 2 3	Vid incidenter eller misstanke om brott ska samverkan ske med chef för berörd verksamhet, juridikenheten, HR-enheten och säkerhetsenheten. Polisanmälan och insamling av bevis m. m. ska ske i samråd mellan dessa parter.
I 11.6 0 1 2 3	Vid incidenter av sådan dignitet att den påverkar kommunens förmåga att bedriva verksamhet eller innebär allvarliga konfidentialitetsbrister ska den it-nära verksamheten omedelbart rapportera till Tjänsteman i beredskap hos Säkerhetsenheten.

5.11.1 Krisorganisation och krisplan

Det ska finnas en krisplan som kan aktiveras vid allvarliga incidenter eller kriser (major incidents) i it-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bl.a. krisorganisation, kontaktpersoner och operativa steg under en allvarlig störning eller kris.

ID	Regler och anvisningar för krisorganisation och krisplan
I 11.7 0 1 2 3	Det ska finnas en krisorganisation på LKDATA för allvarliga incidenter och kriser, vilken tydligt beskriver roller och ansvar.
I 11.8 0 1 2 3	Det ska finnas en krisplan för LKDATA som ska aktiveras vid en allvarlig incident eller kris. Krisplanen ska bl.a. innehålla krisorganisation, kontaktpersoner och operativa steg under en allvarlig störning eller kris.
I 11.9 0 1 2 3	Krisplanen ska testas och övas minst en gång per år. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för it.

5.12 Kontinuitetshantering

Kontinuitetshantering innebär ett systematiskt arbete med att dels skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser, dels minimera konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar identifiering av kritiska it-komponenter samt deras beroende av stöd från andra it-komponenter och resurser, t.ex. personal och lokaler.

Ansvar för kontinuitetshantering		Fördjupad information
●	Objektägare it ansvarar för att kontinuitetsplaner finns för it-komponenter som ingår i förvaltnings-objekten. För kontinuitetsplanering av övriga it-komponenter som hanteras av LKDATA ansvarar CIO.	Kapitel 4.2 – Verksamhetsnära roller och ansvar Kapitel 4.13 – Kontinuitets-hantering Kapitel 5.2 – It-nära roller och ansvar

Kritiska verksamhetsprocesser kan ibland vara helt beroende av att it-komponenter finns tillgängliga och fungerar som avsett. Kontinuitetshantering för it är därför en viktig del av informationssäkerhetsarbetet för att minimera negativa konsekvenser vid allvarliga it-relaterade incidenter eller avbrott. Syftet är att skyndsamt kunna återgå till ett normalläge efter ett större avbrott, så att konsekvenserna för verksamheten blir så lindriga som möjligt.

Det måste finnas en beredskap för hur kommunen hanterar kontinuitet för it-komponenter med förhöjda och höga skyddsbehov vad gäller tillgänglighet. Objektägare it ansvarar för att kontinuitetsplaner finns på plats och att dessa motsvarar de krav som finns för olika objekt. Planerna ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på LKDATA. En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering (se kapitel 5.7 – It-driftsäkerhet).

ID	Regler och anvisningar för kontinuitetshantering
I 12.1 2 3	Kontinuitetsplaner ska finnas för samtliga kritiska it-komponenter med förhöjda eller höga skyddsbehov vad gäller tillgänglighet.
I 12.2 0 1 2 3	Kontinuitetsplanerna ska övas, testas och utvärderas regelbundet. Identifierade brister och svagheter ska åtgärdas med syfte att ständigt förbättra tillgänglighet för it-komponenterna.
I 12.3 0 1 2 3	Kontinuitetsplanerna ska finnas tillgängliga för de medarbetare som utför aktiviteterna. Samtidigt utgör planerna i sig information med förhöjda skyddsbehov och ska därför förvaras skyddade så att de inte är åtkomliga för obehöriga.

5.13 Granskning och kontroll

Säkerheten för olika it-komponenter ska granskas regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig skyddsnivå upprätthålls. Granskning kan genomföras som granskning av systemets design och egenskaper. Det kan också innebära skanning av sårbarheter med automatiserade verktyg eller s.k. penetrationstester. Det är särskilt viktigt med kontroll och granskning när nya it-system och it-tjänster införs.

Ansvar för granskning och kontroll av it-komponenter		Fördjupad information
●	Informationssäkerhetssamordnaren tillsammans med it-säkerhetssamordnaren och informationssäkerhetsrådet ansvarar för att granskning och kontroll sker av kommunens it-komponenter.	Kapitel 3.4.1 – Informations-säkerhetssamordnaren Kapitel 3.4.3 – Informations-säkerhetsrådet Kapitel 5.2.3 – It-säkerhetssamordnare

Kommunens it-miljö vad gäller informationssäkerhet ska revideras minst vart fjärde år.

ID	Regler och anvisningar för granskning och kontroll
I 13.1 	It-komponenter med förhöjda eller höga skyddsbehov ska regelbundet granskas och kontrolleras för att sårbarheter och brister ska upptäckas.
I 13.2 	Vid införande av nya och förändring av it-komponenter ska en granskning genomföras för att säkerställa att it-komponenten uppfyller de säkerhetskrav som ställs. Granskningen ska genomföras och godkännas innan driftstart får ske. Granskningen kan vid behov komplett-eras med penetrationstester vid misstanke om bristande säkerhet.
I 13.3 	Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i objektplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart.
I 13.4 	Rapportering av sårbarheter och brister som kan ge kommunen betydande konsekvenser ska ske till informationssäkerhetsrådet.
I 13.5 	Kommunens it-miljö ska revideras minst vart fjärde år vad gäller informationssäkerhet. Innan en sådan revision kan ske ska följande beaktas: ● Behov av åtkomst till system och data inför revision ska avtalas med objektägare verksamhet. Omfattningen av tekniska aktiviteter för revision ska beskrivas för och godkännas av it-komponentens ägare. ● Aktiviteter vid revision ska om möjligt begränsas så att information i de system som testas inte påverkas eller röjs. ● Revision som kan påverka tillgänglighet bör utföras under ett servicefönster eller vid en tidpunkt när verksamheten påverkas så lite som möjligt. ● All åtkomst vid revision ska övervakas och loggas.

Kapitel 6 -
Informationssäkerhet och fysiskt skydd

6.1 Inledning

I detta kapitel finns regler och anvisningar som gäller fysiskt skydd kopplat till informationssäkerhet i Linköpings kommun. Fysisk informationssäkerhet är en del av den tekniska säkerhet som likt it-säkerhet syftar till att skydda information. Det handlar i stora drag om att

- säkerställa åtkomst till information och utrustning
- upprätthålla informationens konfidentialitet
- se till att informationen inte förändras eller förstörs

Fysisk informationssäkerhet relaterar ofta till faktiska fysiska skydd, mekanismer eller funktioner, och utformningen av fysiska skyddsåtgärder ska i möjligaste mån följa kända och tillämpade referenser, vedertagna normer eller svensk standard. Hänvisningar till andra vägledningar och referenser används i kapitlet när så är möjligt.

Gäller endast utrymmen där information hanteras

Regler och anvisningar i detta kapitel gäller fastigheter, lokaler och utrymmen där informationshantering sker eller information lagras eller där information används för kommunens verksamhet.

Det betyder generellt att kraven och rekommendationerna framför allt riktas mot just dessa typer av utrymmen – inte mot närliggande eller omkringliggande utrymmen eller områden. Regler och anvisningar gäller exempelvis utrymmen där

- medarbetare vid social och omsorgsförvaltningen arbetar med utredningar
- sjuksköterskor på ett äldreboende arbetar med administration
- skolpersonal utför administration
- förvaltningar arbetar med t.ex. ansökningshandlingar
- särskilda utrymmen hos LKDATA

Här avses alltså generellt sett inte de utrymmen och områden som ligger i närheten av eller anslutning till dessa utrymmen eller utrymmen där allmänheten kan befinna sig, t.ex. bibliotek, badhus, matsalen i ett äldreboende eller en skolkorridor

- I detta kapitel används i huvudsak två fysiska skyddsnivåer som utgångspunkt: Basnivåskydd: Med basnivåskydd menas att skyddet ska tillämpas i de flesta av kommunens förvaringar, lokaler och utrymmen.
- Förstärkt skydd: Med förstärkt skydd menas att skyddet ska tillämpas där skyddsvärd information (förhöjda eller höga skyddskrav) hanteras i någon form eller där det finns uttryckliga krav eller förväntningar på implementerade fysiska skydd.

6.2 Allmänt om säkerhet och fysiskt skydd

Ofta krävs att man ser till en helhet för att uppnå god informationssäkerhet med fysiska skydd. Enskilda skyddsåtgärder – t.ex. att förstärka en dörr, installera ett inbrottslarm eller sätta galler på ett fönster – kan vara onödigt eller rentav felaktigt, om det inte finns ett tydligt mål med åtgärden. För att undvika att säkerhetsarbetet blir otydligt och endast löser akuta

situationer måste det därför finnas en systematik i arbetet. Man behöver ha en helhetssyn och ett systematiskt förhållningssätt tillsammans med andra näraliggande områden t.ex brandsskyddsarbete och arbetsmiljöarbete.

Informationsruta

Grundregel för fysiskt skydd
En bra grundregel är att aldrig lämna information oskyddad om den bedöms som skyddsvärd ur något informationssäkerhetsperspektiv. Utrustning som i sig är skyddsvärd eller som behandlar skyddsvärd information bör placeras dels så att tillträde till utrustningen minimeras, dels så att utformningen av lämpliga skyddsåtgärder underlättas.

Planeringen av fysiskt skydd ska inte bara handla om byggnadstekniska aspekter som utformning av väggar, fönster och dörrar utan även inkludera faktorer som t.ex. hur byggnaden bäst skyddas mot fysiska och miljömässiga hot. Om det är motiverat ska även en riskanalys göras, t.ex. om byggnation planeras i närheten, om närliggande verksamheter hanterar brandfarliga eller explosiva varor eller om hot som kan tänkas riktas mot verksamheter i närområdet.

Informationsruta

Riskanalysen är ett centralt verktyg inom fysiskt skydd
Eftersom det fysiska skyddet påverkas av omkringliggande faktorer är riskanalysen det verktyg som kan identifiera vilka lämpliga skyddsåtgärder som behöver vidtas. Nivån på det fysiska skyddet bör alltid baseras på genomförda riskanalyser och stå i proportion till de risker som identifieras.

Den juridiska person som är informationsresursägare inom det fysiska området är vanligen en lokal- eller fastighetsägare. Det är den rollen som delges skyddsbehov från informationsägaren, oftast via en lokal verksamhetschef. Det är verksamhetschefen som har ansvaret att verkställa skyddsbehovet i samråd med resursägaren. (Se även kapitel 4 – Informationssäkerhet i verksamhetsnära förvaltning.)

Ansvar som informationsresursägare		Fördjupad information
●	Informationsresursägare inom det fysiska området ansvarar för att verkställa det skyddsbehov som informationsägaren uttryckt.	Kapitel 4 – Informationssäkerhet i verksamhetsnära förvaltning

6.3 Områden för styrning av fysiskt skydd

Fysiskt skydd består av flera nivåer. För den fysiska informationssäkerheten inom Linköpings kommun ingår regler och anvisningar för följande områden:

- områdesskydd

- skalskydd och säkerhetszoner
- tillträde till utrymmen
- särskilt skyddsvärda utrymmen (arkiv, datahallar, teleutrymmen etc.)
- brandskydd
- skydd av utrustning
- bevakning

Vidare gäller benämningen utrymme alla typer av fastigheter, lokaler, rum, ytor som används av kommunen.

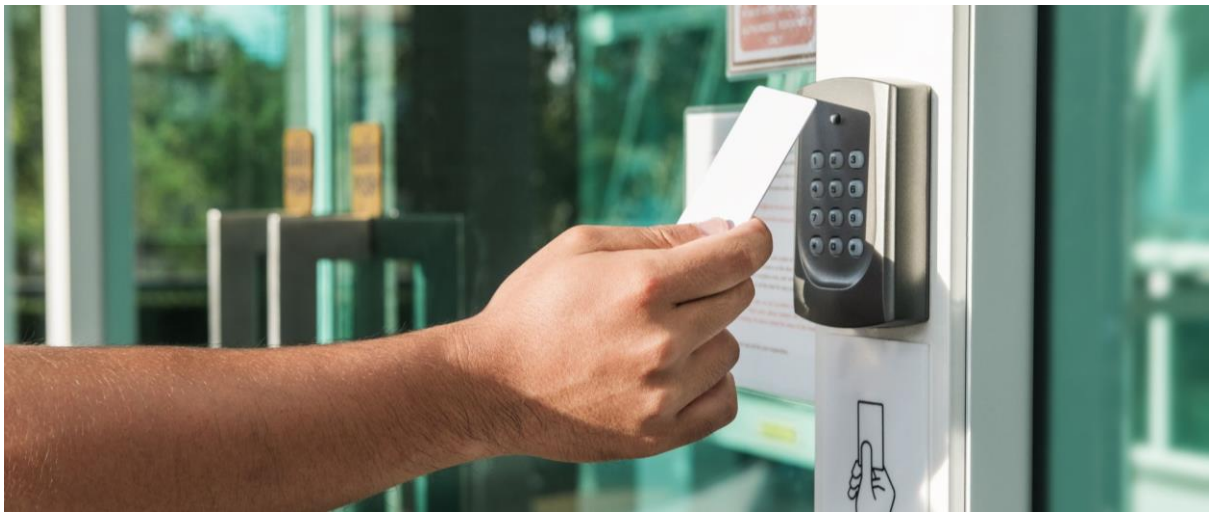


Bild: Bilden visar en hand som scannar ett kort mot en portkodsscanner.

Exempel

Använd riskanalys och utforma det fysiska skyddet proportionerligt. Om skyddsvärd information exempelvis förvaras högt upp i en byggnad, i en inre säkerhetszon som kräver flera inpasseringar genom förstärkta och larmade skalskydd, är det sannolikt inte nödvändigt att införskaffa ett inbrottsklassat dokumentskåp även om reglerna uttryckligen anger detta.

6.4 Områdesskydd

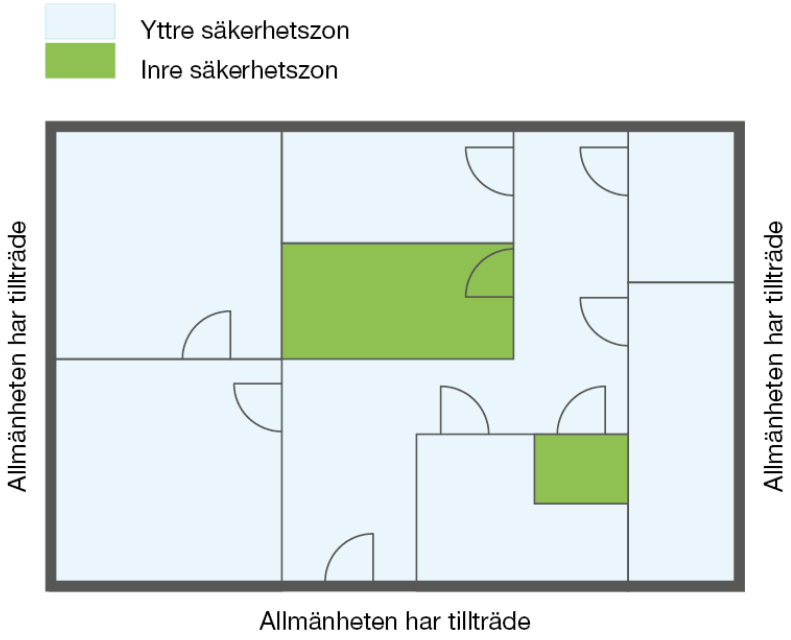
Med områdesskydd menas vanligen staket eller grindar som avgränsar ett specifikt område utanför ett utrymme. Ett områdesskydd kan även kompletteras med elektroniska skydd, t.ex. kameraövervakning. (Anvisningar för utformning av områdesskydd återfinns delvis i SSF Stöldskyddsföreningens standard SSF 200.)

ID	Regler och anvisningar för områdesskydd
F 4.1 0 1 2 3	Behovet av områdesskydd ska beslutas efter en riskanalys för aktuellt utrymme.

6.5 Skalskydd och säkerhetszoner

Skalskydd är en gräns i ett utrymmes omslutningsyta (golv, väggar och tak) som har ett fysiskt skydd som försvårar forcering och obehörigt tillträde. Skalskydd kan delas upp i mekaniskt skydd (t.ex. lås), elektroniskt skydd (t.ex. larm) samt bevakning.

Genom att använda skyddsbarriärer i en fastighet finns möjlighet att förbättra skyddet. Skyddsbarriärer kan då bilda säkerhetszoner (områden eller skikt) som försvårar tillträde till skyddsvärd information. Säkerhetszoner är antingen av inre eller yttre typ. Utanför den yttre säkerhetszonen har vanligen allmänheten tillträde. En inre säkerhetszon angränsar till andra inre säkerhetszoner eller till en yttre säkerhetszon.



Figur 30. Visar en bild på ett fyrkant indelad i olika sektioner, föreställande ett Utrymme indelat i olika säkerhetszoner. Två utav åtta sektioner är grönmarkerade.

Ibland är det inte möjligt att uppfylla skyddskraven helt, eftersom olika omständigheter eller förutsättningar skapar faktiska begränsningar. Om så är fallet ska kompenserande skyddsåtgärder alltid övervägas, t.ex. larm, övervakning eller andra typer av skydd.

Flera barriärer kan erbjuda tillräckliga fysiska skydd
Underskatta inte betydelsen av att införa naturliga barriärer i utrymmen. Arbetsplatser kan t.ex. placeras så att det skapas en naturlig in- och utpassering till utrymmen där skyddsvärd information hanteras. Genom smart planering är det ofta möjligt att tillfredsställa höga skyddsbehov.

Alla utrymmen som används av Linköpings kommun ska bedömas utifrån värdet på den information som hanteras eller lagras i utrymmet. Innanför skalskyddet ska kommunens utrymmen sektioneras så att skyddsvärda informationsresurser får förstärkt skydd.

Säkerhetsskåp kan utgöra ett ytterligare skydd och bör användas för information med högt skyddsbehov när skyddet inte kan uppnås på annat sätt. Det ska finnas hanteringsregler för säkerhetsskåp som styr behörigheter, koder och nycklar för de skåp som används. Om flera personer har tillgång till samma säkerhetsskåp bör alla användare vara behöriga till all information i säkerhetsskåpet. Det ska finnas huvudnycklar/koder som gör att informationen alltid kan tas fram av behöriga personer.

ID	Regler och anvisningar för skalskydd och säkerhetszoner
F 5.1 0 1 2 3	Alla utrymmen som kommunen använder ska bedömas utifrån värdet på den information som hanteras eller lagras i utrymmet. Omfattning av skalskydd enligt regel F5.2–F5.6 ska alltid föregås av en riskanalys som avgör om dessa utrymmen behöver skydd.
F 5.2 0 1 2 3	Som basnivå för skalskydd av kommunens utrymmen bör följande tillämpas: ● mekaniskt skydd enligt SSF 200 skyddsklass 1 ● inbrottslarmsystem enligt SSF 130, larmklass 1 med kompletterande försåtsskydd. Eventuell larmöverföring bör vara övervakad och ansluten till ständigt bemannad larmmottagare. Kompenserande skyddsåtgärder bör vidtas vid behov.
F 5.3 2 3	Vid behov av förstärkt skalskydd hos kommunens utrymmen bör följande tillämpas: ● mekaniskt skydd enligt SSF 200 skyddsklass 2 eller 3 ● inbrottslarmsystem enligt SSF 130, larmklass 2 eller 3. Eventuell larmöverföring bör vara övervakad och ansluten till ständigt bemannad larmmottagare. Kompenserande skyddsåtgärder bör vidtas vid behov.
F 5.4 2	Hantering av information med sekretess bör alltid ske i utrymmen enligt F5.2.
F 5.5 3	Hantering av information med stark sekretess bör alltid ske i utrymmen enligt F5.3.
F 5.6 3	Hantering av information med stark sekretess bör ske i inre säkerhets-zon. Om hantering sker i yttre säkerhetszon ska kompenserande skyddsåtgärder vidtas.

Byggnation och skalskydd ska ses som en helhet med gemensam skyddsnivå. Varje komponent i skyddet ska planeras så att beslutad säkerhetsnivå kan upprätthållas. Verksamhetens instruktioner för fysiskt skydd ska därför alltid användas vid byggnation, ombyggnation och andra liknande aktiviteter som kan påverka skyddet. Behov av skyddsåtgärder ställs av informationsägare och riktas till berörd chef (se även kapitel 4 – Informationssäkerhet i verksamhetsnära förvaltning) som vidarebefordrar detta till informationsresursägare.

6.6 Tillträden till lokaler och utrymmen

Vem som får tillträdet till utrymmen som används av Linköpings kommun ska regleras.

Reglerna för externa parter (t.ex. vid service, underhåll eller reparation) ska följa kommunens regler och anvisningar för besökande (se kapitel 2 – Informationssäkerhet för medarbetare). I särskilda situationer eller vid särskilda behov kan skriftliga dokument (signering av blankett för tystnadsplikt) upprättas.

ID	Regler och anvisningar för tillträde till lokaler och utrymmen
F 6.1 0 1 2 3	Tillträde till de utrymmen som kommunen använder ska endast ges medarbetare som behöver tillträde utifrån sin roll och sina arbetsuppgifter. Tillämpning av tillträde enligt regel F6.2 till F6.5 ska alltid föregås av en riskanalys som avgör om tillträdet till dessa utrymmen behöver regleras.
F 6.2 0 1 2 3	Särskilda rutiner ska finnas för att hantera tillträde för besökare[20].
F 6.3 0 1 2 3	En besökare får aldrig lämnas ensam i ett utrymme som hanterar eller lagrar information som har förhöjt skyddsbehov eller därutöver.
F 6.4 0 1 2 3	Alla utrymmen som kommunen använder bör förses med passer-kontrollsystem. En riskanalys ska avgöra skyddsbehov och typ av passerkontrollsystem.
F 6.5 3	För utrymmen där information med högt skyddsbehov hanteras bör passerkontrollssystem finnas. Detta system bör ha förutsättningar för och tillämpa spårbarhet på personlig nivå.
F 6.6 0 1 2 3	För mekaniska nycklar bör huvudnyckelsystem undvikas. Centralt viktiga nycklar bör förvaras i nyckelskåp med tillträdeskontroll.

[20] Här avses främst externa besökare som inte är anställda av kommunen.

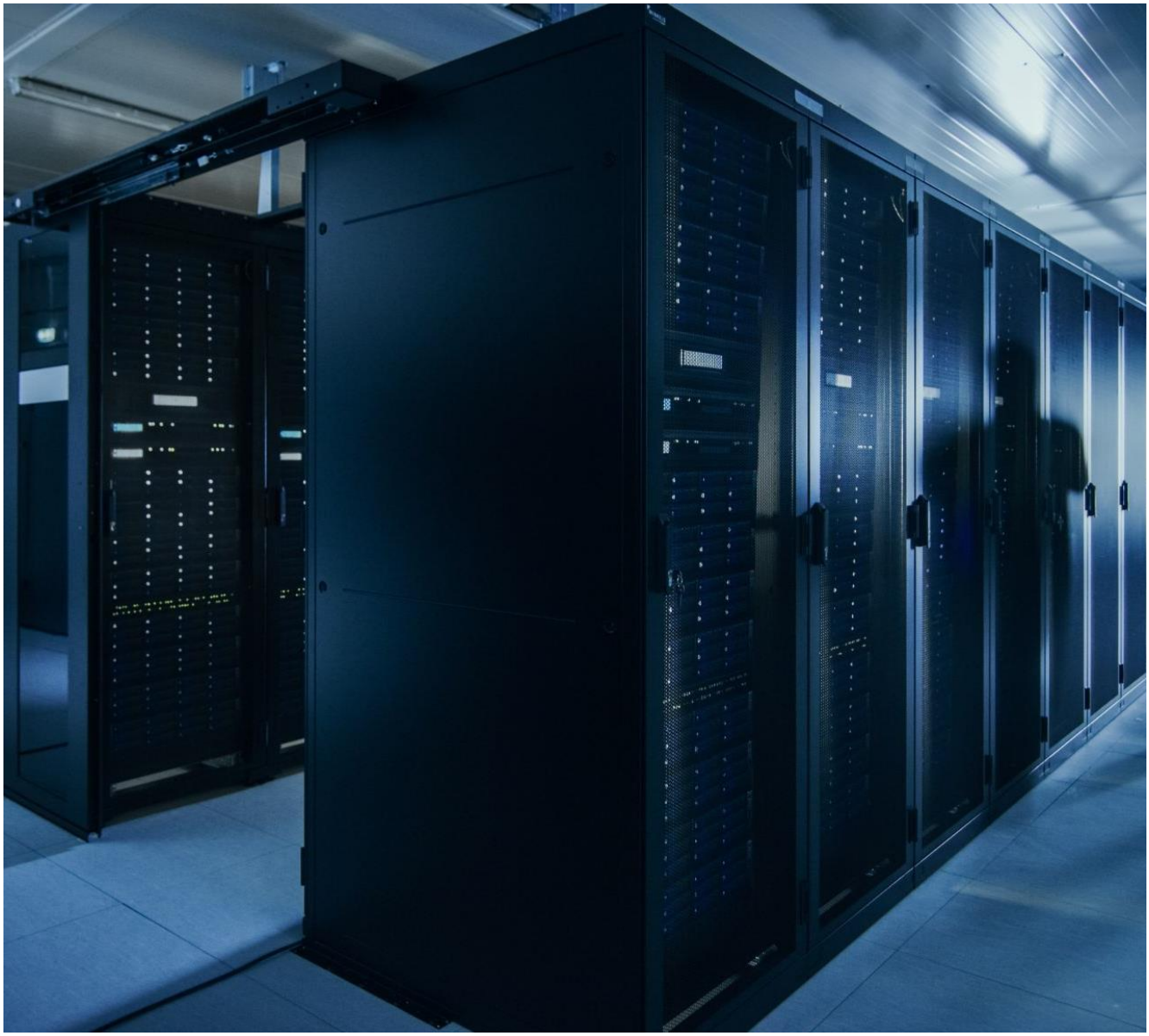


Bild: Bilden visar ett serverrum med en skuggreflektion av en människa

6.7 Särskilt skyddsvärda utrymmen

Särskilt skyddsvärda utrymmen ska utformas enligt särskilda instruktioner. Dessa utrymmen ska vara förtecknade och säkerhetschefen är ansvarig för denna förteckning. Exempel på sådana utrymmen är arkivlokaler, it-utrymmen, datorhallar, televäxelutrymmen, kommunikationsnoder eller andra typer av korskopplingsutrymmen samt utrymmen för förvaring av säkerhetskopior.Dessa instruktioner gäller även leverantörer av externa utrymmen där kommunens information hanteras men där kommunen inte har någon egen verksamhet.

Det finns sex typer särskilt skyddsvärda utrymmen i Linköpings kommun:

- Datorhallar. Med en datorhall menas ett utrymme som förvarar en större mängd it-komponenter. En datorhall är initialt avsedd och projekterad för it-drift. Den är därtill kritisk för upprätthållande av funktioner i kommunens infrastruktur och har höga krav gällande tillgänglighet.
- Kommunikationsnod typ A. Här menas ett utrymme som innehåller utrustning för datakommunikation som är ansluten till kommunens huvudring (fiberring). En typ A-nod kan mata typ B-, typ C- och typ D-noder. En typ A-nod är kritisk för att upprätthålla funktioner i kommunens nät och har höga krav gällande tillgänglighet.
- Kommunikationsnod typ B. Här menas ett utrymme som innehåller utrustning för datakommunikation som är ansluten till en typ A-nod. En typ B-nod kan mata typ C- och typ D-noder. En typ B-nod är inte kritisk för kommunens nät och har lägre krav gällande tillgänglighet än en typ A-nod.
- Kommunikationsnod typ C. Här menas ett utrymme som innehåller utrustning för datakommunikation som är ansluten till en typ A- eller en typ B-nod. En typ C-nod kan endast mata typ D-noder. En typ C-nod är inte kritisk för kommunens nät och har lägre krav gällande tillgänglighet än en typ A- och en typ B-nod.
- Kommunikationsnod typ D. Här menas ett utrymme/skåp som innehåller utrustning för lokalt fastighetsnät. En typ D-nod ansluter ändutrustning som t.ex. datorer, skrivare, trådlösa accesspunkter. En typ D-nod är en ändnod och matar inte vidare till annan nod.
- Arkiv, utrymmen för att lagra framför allt pappersbunden information. Linköpings kommun har arkiv för både korttids- och långtidslagring av pappersbunden information. Den fysiska säkerheten i kommunens arkiv ska följa de föreskrifter som återfinns i svensk lagstiftning, rekommendationer från Riksarkivet samt kommunens arkivreglemente.

(Mer detaljerad vägledning för fysiskt skydd i särskilt skyddsvärda utrymmen återfinns i ett separat dokument, se kapitel 7.2. – Länkar och referenser.)

ID	Regler och anvisningar för särskilt skyddsvärda utrymmen
F 7.1 0 1 2 3	Alla kommunikationsnoder och liknande utrymmen som kommunen använder ska utformas enligt vägledningen Fysiska skydd i särskilt skyddsvärda utrymmen (Se kapitel 7.2 – Länkar och referenser).
F 7.2 0 1 2 3	Alla datorhallar som kommunen använder ska utformas enligt vägledningen Fysiska skydd i särskilt skyddsvärda utrymmen (Se kapitel 7.2 – Länkar och referenser).
F 7.3 0 1 2 3	Säkerhetskopior av information ska inte förvaras i samma utrymme som den it-utrustning den kopierar utan bör förvaras minst två kilometer från den utrustning den kopierar. Skåp eller motsvarande förvaring ska vara klassad för brandskyddad datamediaförvaring enligt lägst brandskyddsklass S60DIS samt inbrottsklassad enligt SS3492 eller motsvarande.
F 7.4 0 1 2 3	Arkivlokaler ska utformas i enlighet med Riksarkivets föreskrift RA-FS 2013:4 – Riksarkivets föreskrifter och allmänna råd om arkivlokaler.
F 7.5 0 1 2 3	Skyddsvärd information ur konfidentialitets- och tillgänglighets-perspektiv som förvaras i kommunens verksamheter bör förvaras i dokumentskåp som har lägst brandskyddsklassning S60P och inbrottsklassning SS3492 eller motsvarande.
F 7.6 0 1 2 3	Särskilda instruktioner ska upprättas för samtliga särskilt skyddsvärda utrymmen. Externa parter som utför arbeten i särskilt skyddsvärda utrymmen ska få instruktioner om vilka regler som gäller innan tillträde godkänns. För exempel på lämpliga rutiner, se Linweb.
F 7.7 0 1 2 3	För respektive särskilt skyddsvärt utrymme ska det utses en ansvarig för upprätthållande av den fysiska informationssäkerheten. Respektive verksamhetschef beslutar om vem som ska ha ansvaret.

6.8 Brandskydd

Bild: Bilden visar en brandman som står på knä och släcker en eldsvåda

Informationsruta

Ett bra brandskydd är viktigt
Pappersdokument, datorer och annan elektronisk utrustning som exempelvis lagringsmedia är vanligen känsliga för brand, temperaturökningar eller rökgaser. Det är viktigt att det finns lämpliga brandskydd i utrymmen där pappersdokument och utrustning förvaras.

Alla byggnader och anläggningar ska ha ett skäligt brandskydd enligt lagen om skydd mot olyckor. MSB har tolkat att detta innebär att verksamheten ska bedriva ett systematiskt brandskyddsarbete (SBA). Det betyder att det ska finnas ett systematiskt brandskyddsarbete för samtliga byggnader och utrymmen, dock i varierande omfattning. Brandskyddet ska särskilt beaktas för särskilt skyddsvärda utrymmen (se kapitel 6.7 – Särskilt skyddsvärda utrymmen).

Det ska finnas instruktioner som närmare beskriver hur regler och rekommendationer inom SBA tillämpas inom Linköpings kommun. Ägare och nyttjanderättshavare är ansvariga för det systematiska brandskyddsarbetet.

ID	Regler och anvisningar för brandskydd
F 8.1 0 1 2 3	Brandskydd ska bedömas särskilt för alla utrymmen som lagrar eller behandlar information. Brandskydd ska i dessa fall ingå som en del av riskanalysen.
F 8.2 2 3	Om det finns förhöjda eller höga skyddsbehov vad gäller tillgänglighet ska information som lagras i pappersform eller elektroniskt på datamedia förvaras i brandklassade skåp som är anpassade för aktuellt media.

6.9 Skydd av utrustning och skydd i utrymmen

Den utrustning som Linköpings kommun använder i sin informationshantering ska skyddas så att den inte förloras, stjäls eller på annat sätt skadas. Information som hanteras i utrustningen får inte heller förvanskas eller komma i orätta händer. Detta gäller oavsett om utrustningen förvaras i Linköping kommuns egna utrymmen eller utanför dessa. Särskilda instruktioner ska upprättas för hantering av information utanför kommunens egna utrymmen. Se även kapitel 2.13 – Hanteringsregler för olika konfidentialitetsklasser som innehåller regler och anvisningar för hantering av utrustning.

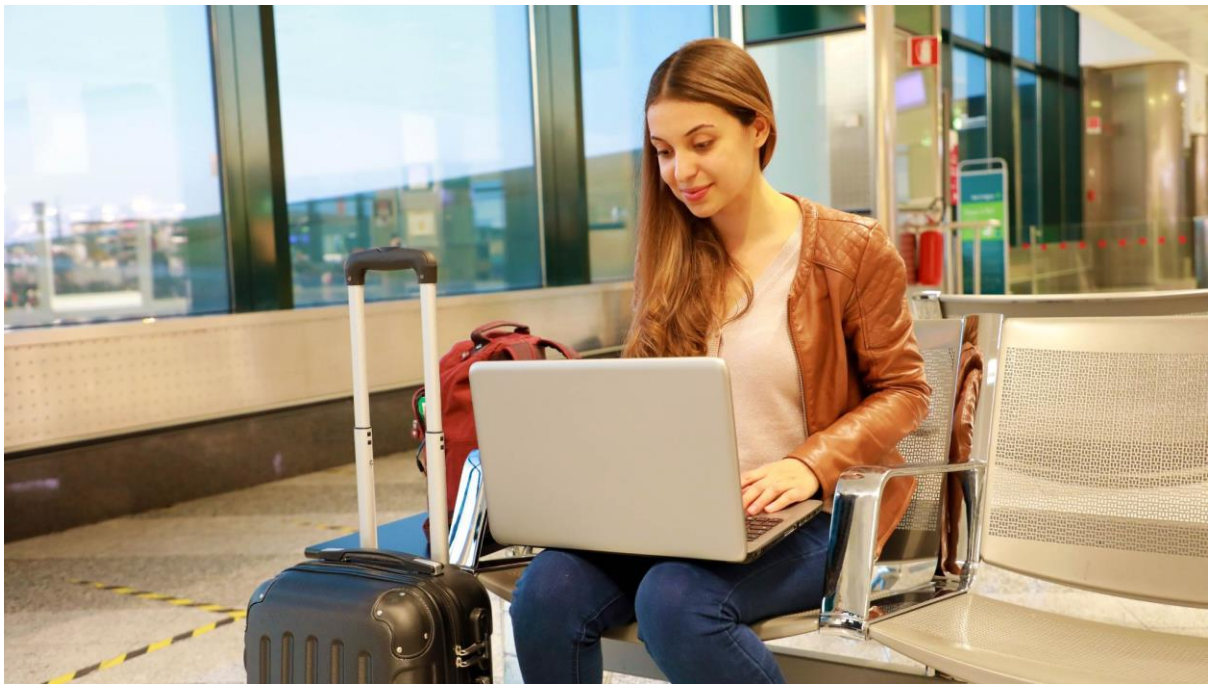


Bild: Bild visar en kvinna som sitter på en flygplats med bagage och en bärbar dator i knät.

Risker utanför kommunens utrymmen

Tänk på att risker vanligen ökar när medarbetare hanterar utrustning utanför de egna lokalerna. Detta gäller alla bärare av information i vid mening men framför allt bärbara datorer, surfplattor, mobiltelefoner och pappersdokument. Var noggrann och håll din information och utrustning under uppsikt eller använd lämpligt fysiskt skydd.

Inredning och placering av utrustning ska ske så att utrustningen skyddas mot fysiska och miljömässiga hot. Skydd ska även finnas mot otillbörlig åtkomst. Kring utrustning som klassats som särskilt skyddsvärd ska lämpligt skydd i enlighet med Linköping kommuns instruktioner implementeras.

För att utrustningen ska kunna fungera som avsett krävs ett antal stödjande funktioner, t.ex. kraftförsörjning, klimatanläggningar, övervakning och monitorering. Dessa funktioner ska underhållas och granskas regelbundet så att de uppfyller de krav som ställs av relevanta interna och externa kravställare, t.ex. tillverkare.

Underhåll, reparation, avveckling och återanvändning av utrustning ska regleras i instruktioner och anvisningar. Denna reglering ska särskilt beakta hur skyddsvärd information hanteras.

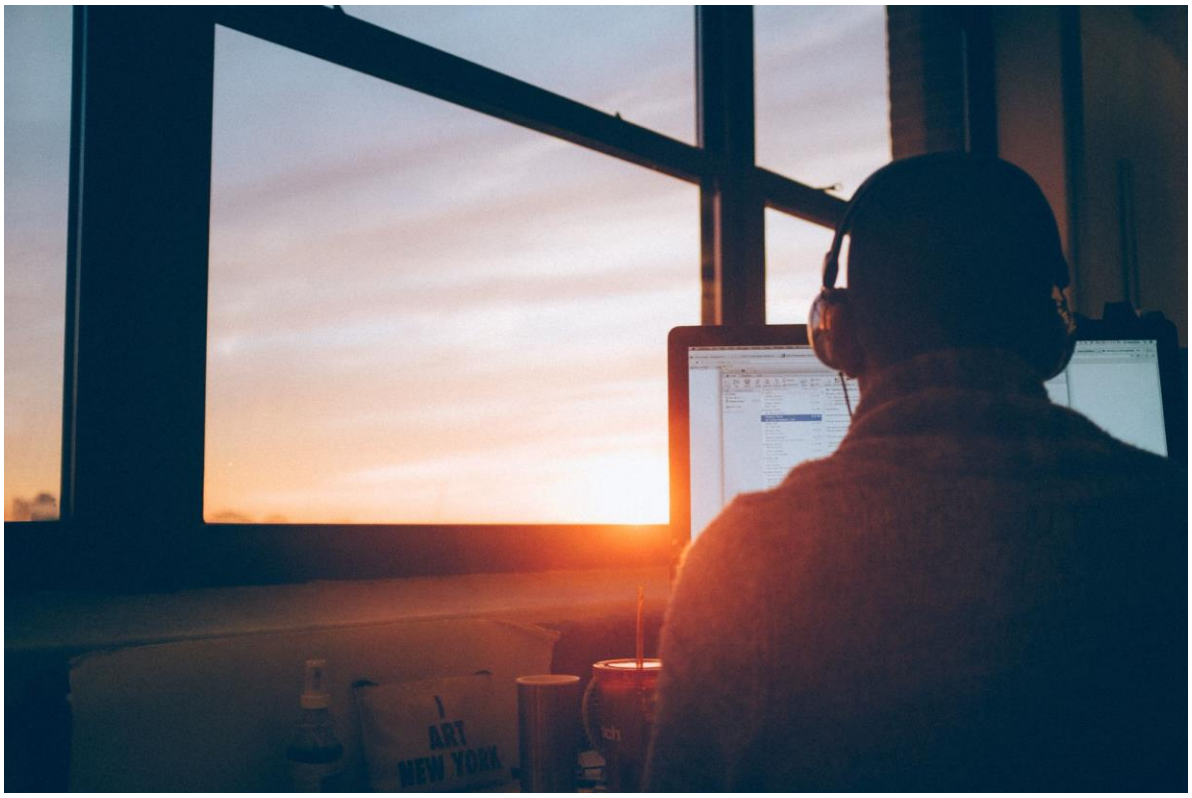
ID	Regler och anvisningar för skydd av utrustning
F 9.1 0 1 2 3	Utrustning ska placeras och skyddas mot stöld och miljömässiga hot, t.ex. värme, kyla eller fukt.
F 9.2 0 1 2 3	Om stationär utrustning är placerad så att det finns en uppenbar risk att utrustningen stjäls eller påverkas negativt bör utrustningen förses med stöldskydd och märkning.
F 9.3 0 1 2 3	Uttag till data- och telefonnät i kommunens utrymmen bör endast vara aktiverade om uttagen används.
F 9.4 2 3	Om utrustning lagrar eller hanterar sekretess eller stark sekretess information ska utrustningen förvaras inlåst eller under personlig uppsikt.
F 9.5 0 1 2 3	Vid underhåll och reparation av utrustning ska åtgärder vidtas så att information inte röjs, flyttas, döljs eller raderas. Om utrustning lagrar information med stark sekretess som ska hanteras av extern part ska särskilda säkerhetsinstruktioner följas.
F 9.6 0 1 2 3	Vid avveckling eller utrangering av utrustning ska åtgärder vidtas så att information inte röjs, raderas, skrivas över eller destrueras. Om utrustning lagrar information med stark sekretess som ska hanteras av extern part ska särskilda säkerhetsinstruktioner följas.

6.10 Bevakning

Bevakning är ett komplement till övriga skyddsåtgärder och kan användas utanför och innanför Linköpings kommuns skalskydd. Krav ska ställas på den gemensamma bevakning som sker av en fastighet, så att bevakningen tillgodoser kommunens skyddsnivåer och skyddsbehov. Vid användning av externa parter (t.ex. kontrakterade bevakningsorganisationer) ska reglering ske genom tydliga villkor, bl.a. vad gäller insatstider, krav på personkontroll av bevakningspersonal samt utbildning i Linköping kommuns säkerhetsinstruktioner för de utrymmen som ska bevakas. Om du har frågor gällande bevakning, kontakta säkerhetsenheten.

ID	Regler och anvisningar för skydd av utrustning
F 10.1 	Utrustning ska placeras och skyddas mot stöld och miljömässiga hot, t.ex. värme, kyla eller fukt.
F 10.2 	För alla utrymmen som lagrar och förvarar information med stark sekretess ska bevakning med ronderande väktare alltid övervägas.
F 10.3 	I anslutning till utrymmen där information med stark sekretess lagras och förvaras bör kameraövervakning övervägas. Riskanalys ska utföras och avgöra behovet av kameraövervakning. Konsultera alltid kommunens säkerhetsenhet före beslut och tillämpning av kameraövervakning.

Kapitel 7 -
Begrepp och referenser



7.1 Begrepp och definitioner

Begrepp	Definition
Administrativa konton	I inloggningskonton med kraftfulla (priviligierade) behörigheter, vilket medför att de personer som har denna behörighet kan utföra nästan alla aktiviteter i ett it-system.
Ansvarig	Person eller funktion inom organisationen som har en roll att antingen genomföra vissa specifika aktiviteter eller följa upp att vissa specifika aktiviteter blir genomförda.
Anvisning	Upplysning om på vilket sätt något ska göras.
Användare	Person eller system som nyttjar informationstillgångar. Kan vara extern eller intern. Kommentar: Ofta menas en person som direkt interagerar med ett datoriserat system. Här förutsätts som regel att användaren har behörighet att använda informationstillgångarna.
Allmän handling	Handlingar som förvaras hos ett allmänt organ, t.ex. en statlig myndighet eller en kommun. Tre kriterier ska vara uppfyllda för att det ska röra sig om en allmän handling: 1. Det ska röra sig om en handling enligt tryckfrihetsförordningen. 2. Handlingen ska förvaras hos myndigheten. 3. Handlingen ska vara antingen inkommen till eller upprättad hos myndigheten. Att en handling är allmän är inte detsamma som att den är offentlig.
Arbetsmaterial	Handling som inte är en allmän handling. Kommentar: En handling som inte är slutgiltigt färdigställd och som ännu inte är en allmän handling.
Autentisering	Verifiering av att en användare eller it-resurs är den som den utger sig för att vara.

Begrepp	Definition
Behörig	Person som ingår i en aktuell begränsad gruppering som har en viss rättighet.
Behörighet	Tilldelade rättigheter att använda information eller en resurs på ett specificerat sätt.
Behörighets-kontrollsystem (BKS)	Ett it-system som kontrollerar behörigheter.
CIO	Chief Information Officer. CIO för Linköpings kommun har det övergripande ansvaret för funktionen it och för den it-nära förvaltningen samt tillhörande leverantörsstyrning avseende it-komponenter inom kommunen.
CMDB	Configuration management database, en term som används inom it-förvaltningen (se även ITIL). Avser en databas där information om all it-utrustning lagras.
Data	Representation av fakta i form av t.ex. tecken eller signaler som är lämpade för överföring, tolkning eller bearbetning med hjälp av människor eller automatiska hjälpmedel.
Datamedia	Elektronisk lagringsmedia, t.ex. databand, usb-minne, hårddisk, cd/dvd.
Digital signatur	Ett certifikatbaserat digitalt ID som utfärdats av en ackrediterad certifikatutfärdare (CA) eller leverantör av betrodda tjänster (TSP). När någon undertecknar ett dokument med digital signatur kopplas identiteten unikt till den personen, signaturen är kopplad till dokumentet genom kryptering och allt kan verifieras med underliggande teknik.
Distansarbete	Arbete som sker från en arbetsplats utanför kommunens lokaler. Termen avser numera huvudsakligen arbete hemifrån där man har kontakt med den ordinarie arbetsplatsen via telefon och dator, vanligen via en VPN-tunnel.
Dokument-hanteringsplan	En dokumenthanteringsplan är en förteckning av myndighetens olika handlingstyper (informationstyper) med beskrivning av vad det är för slags handlingar, vem som har ansvar för handlingen, var handlingarna finns samt beslut om gallring av handlingarna. Se även informationshanteringsplan (IHP).

Begrepp	Definition
Driftssäkerhet	Förmågan hos en it-komponent att kunna utföra sin funktion.
Extern användare	Användare som inte är anställd under kommunens organisationsnummer.
Fysiskt skydd	Skydd mot att obehöriga får tillträde till platser där -kommunens information hanteras eller lagras. Även skydd mot att information förstörs vid olyckor, t.ex brand eller översvämning.
Förvaltningsstyrning	Ett arbetssätt för att nå ordning, prioritering och tydligt ansvar i processer för förvaltning av it.
Gruppkonto	Ett inloggningskonto som delas av flera kända personer.
Godkända tjänster	En uppsättning tjänster som godkänts av Linköpings kommun för användning i kommunens it-infrastruktur.
Gästkonto	Ett tillfälligt inloggningskonto som kan tilldelas en person under en begränsad tid.
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten. Kommentar 1: Kan indelas i avsiktliga respektive oavsiktliga hot. Med avsiktliga hot menas hot med illasinnad avsikt. Med oavsiktliga hot menas hot som existerar trots att det saknas en illasinnad avsikt. Kommentar 2: Kan indelas i interna respektive externa hot. Med interna hot menas hot mot säkerheten som orsakas internt. Med externa hot menas hot som har sitt ursprung utanför den egna verksamheten.
Härdning	En metod för att anpassa tillämpning samt förbättra it-säkerhet i it-komponenter. Utförs oftast genom borttag eller anpassning av program/applikationer, samt förändringar av behörigheter och systemparametrar.
Incident	Oönskad händelse som orsakar negativ påverkan. Olika typer av informationssäkerhetsrelaterade incidenter inom kommunen: ● informationssäkerhetsincident ● personuppgiftsincident ● it-säkerhetsincident ● fysisk säkerhetsincident

Begrepp	Definition

Incident manager	Har ansvar för att hantera större incidenter inom it-nära förvaltning. Rollen definieras i standarden ISO/IEC 20000.
Incidenthantering	Hantering av en oönskad händelse.
Information	Innebörd i data, dvs. tolkad data.
Information security manager	Har ansvar för att hantera informationssäkerhetsärenden inom it-nära förvaltning. Rollen definieras i standarden ISO/IEC 20000.
Informations-behandlingsresurs	En enhet för behandling av information i form av t.ex. en person eller en teknisk enhet, t.ex. ett it-system, en it-tjänst eller infrastruktur som hanterar information. Kan även benämnas informationsresurs eller bara resurs.
Informationsbärare	Media som innehåller den informationen som avses, t.ex. papper, magnetband, usb-minne, bild eller teckning.
Informations-hanteringsplan (IHP)	En informationshanteringsplan är en förteckning av myndighetens olika handlingstyper (informationstyper) med beskrivning av vad det är för slags handlingar, vem som har ansvar för handlingen, var handlingarna finns samt beslut om gallring av handlingarna. Den innehåller även information om informationsklassning för varje informationstyp. Se även dokumenthanteringsplan.
Informations-klassning	Analys för att identifiera skyddsbehovet för en viss -informationstyp.
Informationsmängd	Används vanligen synonymt med begreppet informationstyp. Dock kan begreppet även avse en avgränsad samling information som existerar i ett sammanhang. (Se även informationstyp.)
Informations-resursägare	Ägare eller ansvarig för en informationsresurs, t.ex. objektägare it, en lokalansvarig eller en fastighetsägare.
Informationsskada	Ett samlingsbegrepp för negativ påverkan på information om denna har röjts till obehörig, inte är korrekt, inte är tillgänglig eller inte går att spåra.
Informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information.

Begrepp	Definition
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information. Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.

	Kommentar: Informationssäkerhet kan ses som en uppsättning säkerhetsåtgärder för att bevara informationens konfidentialitet, riktighet och tillgänglighet samt spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation. Informationssäkerhet omfattar både organisatorisk, it-teknisk och fysisk säkerhet.
Informations-säkerhetsaspekt	Perspektiv för att bevara informationens konfidentialitet, riktighet, tillgänglighet samt spårbarhet. Se även informationssäkerhet.
Informationssäkerhes-incident	En eller flera oönskade eller oväntade händelser som får negativa konsekvenser för verksamheten och dess informationssäkerhet.
Informationstillgång	Information av värde för organisationen samt de resurser som hanterar den, exempelvis personer, papper, mjuk- vara, hårdvara eller immateriella tillgångar, t.ex. rykte.
Informationsägande nämnd	Den nämnd som har det yttersta ansvaret för att information behandlas korrekt och får lämpligt skydd. Kommentar: En informationsägande nämnd bör uppdra åt en funktion att fullgöra och verkställa ansvaret genom att den utser en informationsägare i respektive förvaltningsorganisation.
Informationsägare	En roll som verkställer en informationsägande nämnds ansvar genom att se till att information behandlas korrekt och får ett lämpligt skydd genom att informationen klassas. Kommentar: Uppdraget omfattar bl.a. informationsklassning (konsekvensvärdering) av informationen samt kontroll av att informationens skyddsåtgärder motsvarar önskad skyddsnivå. Begreppet ägare innebär inte en faktisk äganderätt till informationen.

Begrepp	Definition
It-nära förvaltning	Organisation för förvaltning av it-komponenter (LKDATA).
It-resurs	It-baserad komponent som hanterar information, t.ex. system, verktyg, tjänster eller infrastruktur i form av mjuk- eller hårdvara.
It-system	En tillämpning som består av en eller flera it-komponenter och erbjuder någon form av it-relaterad tjänst.
It-säkerhet	It-relaterade tekniska skyddsåtgärder för att upprätthålla informationssäkerhet.
It-tjänst	En tillämpning som erbjuds av en it-komponent t.ex utskrift, identifiering, lagring.
Kommunens nätverk	Kommunens interna it-nätverk. Inkluderar inte publika delar av detta nätverk, t.ex. kommunens publika -webbplats eller Eduroam. Kan även benämnas kommunens intranät.
Kommunikations-säkerhet	It-säkerhet som innebär skydd vid överföring av data. Kan även betecknas nätverkssäkerhet.
Konfidentialitet	Att något inte tillgängliggörs eller avslöjas för obehörig. Innebär skydd mot obehörig insyn och ingår i informationssäkerhet. Kommentar: Termen sekretess används ofta i legala sammanhang och ges där en delvis annan innebörd än konfidentialitet.
Konsekvens	Resultat av en händelse. Kommentar: En händelse kan få flera konsekvenser. Konsekvenser kan vara såväl positiva som negativa och kan uttryckas både kvalitativt och kvantitativt. Initiala konsekvenser kan eskalera genom att negativa effekter tillkommer i efterhand.
Kontinuitetsplan	En kontinuitetsplan innehåller information som hjälper personalen att veta vad den ska göra vid en störning i en kritisk process eller resurs. Syftet är att kunna upprätthålla verksamheten på en tolerabel nivå och att kunna återställa resursen så fort sommöjligt.
Kontinuitetshantering	Arbetsmomenten i kontinuitetsplanen.

Begrepp	Definition
Kryptering	Kryptering gör information svårläslig för alla som inte ska kunna läsa den. För att göra informationen läslig igen krävs dekryptering. Kryptering och dekryptering uppnås vanligen genom olika algoritmer.
Känsliga personuppgifter	Begrepp som härrör från lagstiftning och innebär uppgifter om etniskt ursprung, politiska åsikter, religös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. I dataskyddsförordningen kallas de här uppgifterna särskilda kategorier av personuppgifter.
Ledningssystem för informationssäkerhet (LIS)	Del av organisationens övergripande ledningssystem, baserad på en metod för verksamhetsrisk som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Logg	Historik över händelser.
Medarbetare	Person som är anställd under kommunens organisationsnummer eller förtroendevald. Inhyrd personal som hanterar kommunens information ska också lyda under samma säkerhetsregler som anställda och kan ur informationssäkerhetsperspektiv betraktas som medarbetare.
Mobil enhet	Bärbara datorer, surfplattor och smarttelefoner samt alla enheter som kan lagra elektronisk information, t.ex. cd/dvd, usb-minnen, portabla hårddiskar och liknande.
Molntjänst	Även kallat datormoln, molnet eller cloudtjänster. It-tjänster som tillhandahålls över internet, i synnerhet funktioner som traditionellt sköts på egna datorer men genom molnet sköts av någon annan. Kan t.ex. gälla tillämpningsprogram, serverprogram eller lagring av data.
Oavvislighet (eng. non-repudiation)	Säkerhetsprincip och funktion som gäller kommunikation med innebörden att avsändandet eller mottagandet av ett givet meddelande inte ska kunna förnekas i efterhand av avsändaren respektive mottagaren. Oavvislighet implementeras ofta med hjälp av digitala signaturer och kan t.ex. användas för att uppnå spårbarhet.
Objektägare verksamhet	Roll (se även pm3) inom kommunens styr- och förvaltningsmodell för it-stöd. Företräder verksamhetssidan.
Objektägare it	Roll (se även pm3) inom kommunens styr- och förvaltningsmodell för it-stöd. Företräder tekniksidan.
Begrepp	Definition

Organisatorisk säkerhet/ organisatoriskt skydd	Organisatoriska säkerhetsåtgärder handlar om det -administrativa säkerhetsarbetet som till exempel tilldel-ning av åtkomsträttigheter, interna rutiner, instruktioner och riktlinjer.
Personalfunktion	Enhet inom kommunen som hanterar personalrelaterade ärenden.
Personuppgifts-incident	En händelse som leder till att personuppgifter kommer i orätta händer, förloras eller uppdateras felaktigt.
pm3 (På maintenance management model)	En förvaltningsmodell för it-stöd som utvecklats av företaget På AB i Stockholm. (se även Linweb).
Policy	Ett politiskt styrdokument som beslutas av kommun-fullmäktige.
Redundans	Dubblering av utrustning för att upprätthålla funktion i händelse av tekniska fel.
Regel	En bestämmelse som måste följas.
Resurs	Enhet som lagrar eller något annat sätt behandlar information.
Resursägare	Den som äger teknik, infrastruktur eller tjänster. Motsvarar rollen objektägare it om resursen ingår i kommunens styr- och förvaltningsmodell för it-stöd.
Riktighet	Information är korrekt, aktuell och fullständig. Kommentar: Inkluderar även skydd mot oönskad förändring.
Risk	En risk föreligger när det samtidigt finns ett hot och en brist. Risker mäts genom kombination av sannolikheten för att en incident ska inträffa och konsekvenserna av den.

Begrepp	Definition
Riskacceptans	Ett beslut att acceptera en kvarstående risk. Beslutet tas av riskägaren.
Riskanalys	Process som identifierar och uppskattar storleken på risker mot verksamheten.
Riskbehandling	Övergripande process för riskanalys och riskvärdering. Kommentar: Kan även kallas riskbedömning.
Riskhantering	Samordnade aktiviteter för att styra och kontrollera en organisation med avseende på risk.
Riskmitigering	Process där en identifierad risk minskas genom att minska dess sannolikhet eller konsekvens.
Riskvärdering	Process där en uppskattad risk jämförs med uppsatta riskkriterier för att avgöra riskens betydelse.
Riskägare	Person eller funktion som ansvarar för och har befogenhet att hantera en risk. Ofta Informationsägare, Objektägare verksamhet eller Objektägare IT. Kommundirektören är alltid yttersta riskägare i kommunen.
RPO (Recovery Point Objective)	Maximal tidsförlust som tolereras relaterat till förlust av data vid ett avbrott. Används vanligen för att definiera hur ofta säkerhetskopiering behöver utföras.
RTO (Recovery Time Objective)	Maximal tid som tolereras för en process att återstarta efter ett avbrott. Används vanligen för att definiera hur lång tid återläsning av en säkerhetskopia tillåts ta.
Samarbetsplattform	Intern eller extern e-tjänst för digital samverkan.
Sekretess	Benämning av en konfidentialitetsklass inom Linköpings kommun. Också ett förbud att röja en uppgift, oavsett om det sker muntligt, genom utlämnande av en handling eller på annat sätt (se även konfidentialitet och jämför).
Skadlig kod	En generisk term för skadliga datorprogram. Virus, trojaner och maskar är typer av skadlig kod.
Skydd	Administrativt, logiskt, tekniskt eller fysiskt hinder.
Skyddsbehov	Ett bedömt behov av skydd som behövs för att en befarad konsekvens inte ska inträffa.Skyddsbehov för en it-komponent utgörs av det maximala värdet på informationsklassning inom varje skyddsaspekt för den information som hanteras i it-komponenten.
Begrepp	Definition
Skyddsnivå	En mängd skyddsåtgärder som bedöms behövas för att

	reducera sannolikheten för att en befarad konsekvens inte ska inträffa.
Skyddsvärd (information	Information som har ett högt värde för verksamheten och därför bör skyddas och bevaras.
Skyddsåtgärder	Identifierad uppsättning åtgärder för att möta risker i en organisation.
Social engineering	Försök att tillskansa sig information genom att utge sig för att vara någon man inte är.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller it-resurs.
Stark sekretess	Benämning av en konfidentialitetsklass inom Linköpings kommun. Även ett begrepp som beskriver det så kallade -omvända skaderekvisitet, nämligen att uppgifter i en allmän handling som huvudregel är sekretessbelagda. För att sådana uppgifter ska kunna lämnas ut måste det stå klart att utlämnandet inte kan anses leda till skada. Ett exempel när stark sekretess tillämpas är för allmänna handlingar inom hälso- och sjukvården som gäller uppgifter om en enskilds hälsotillstånd eller andra personliga förhållande. (se även konfidentialitet).
Sårbarhet	Brist i skyddet av en tillgång eller en säkerhetsåtgärd, där denna brist kan utnyttjas för att realisera ett eller flera hot.
Säker utskrift	Metod för att uppnå tillförlitlig identifiering av den person som begär och hämtar ut en utskrift i en skrivare.
Säkerhetsmål	Beskrivning av vad som ska uppnås som ett resultat av en införd säkerhetsåtgärd.
Säkerhetsnivå	Se skyddsnivå.
Teknisk säkerhet	Del av informationssäkerhet där skyddsåtgärder relaterar till tekniska skydd.
Tillgänglighet	Åtkomst för behörig person vid rätt tillfälle.

Begrepp	Definition
Uppgiftsminimering	Arbetssätt där man agerar restriktivt vid hantering av information i allmänhet.

Verksamhetssystem	Är vanligen knutet till en specifik del eller funktion i en verksamhet. Se också it-system.
Öppen information	Benämning av en konfidentialitetsklass inom Linköpings kommun.

7.2 Länkar och referenser

7.2.1 Stöddokument till informationssäkerhetshandboken

Hantering av Säkerhetsskyddsklassificerad information
Dokument som beskriver hantering av Säkerhetsskyddsklassificerad information.
Ansvarig för dokumentet: säkerhetsskyddschef.

It-tekniska säkerhetskrav gällande it-komponenter
Dokument som beskriver it-tekniska säkerhetskrav för respektive informationsklass.
Ansvarig för dokumentet: CIO.

Fysiska skydd i särskilt skyddsvärda utrymmen
Dokument som beskriver fysiska säkerhetskrav för datorhallar, kommunikationsnoder etc.
Ansvarig för dokumentet: säkerhetschefen.

Mall för informationsklassning
Dokument som beskriver hur informationsklassning utförs i en verksamhet. Ansvarig för dokumentet: säkerhetschefen.

Mall för riskanalys för informationssäkerhet
Dokument som beskriver hur riskanalys för informationssäkerhet utförs i en verksamhet.
Ansvarig för dokumentet: säkerhetschefen.

7.2.2 Lagar och regelverk som relaterar till informationsäkerhet

Allmänna handlingar
Offentlighetsprincipen reglerar vilken typ av information som ska betraktas som allmänna handlingar, vilket framgår av tryckfrihetsförordningens 2 kapitel. Vissa allmänna handlingar innehåller uppgifter som ska omfattas av med sekretess.

- Tryckfrihetsförordning (1949:105)
- Offentlighets- och sekretesslag (2009:400)

Sekretessbelagd information rörande Sveriges (rikets) säkerhet
Information som är sekretessbelagd med hänsyn till rikets säkerhet ges ett särskilt skydd genom säkerhetsskyddslagen. Säkerhetsskyddslagen innehåller bland annat bestämmelser om vilken kontroll man får göra av personer som hanterar den typen av information.

- Säkerhetsskyddslag (2018:585)

Personuppgifter
Dataskyddsförordningen (GDPR) är till för att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Dataskyddsförordningen gäller i

hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.

- Dataskyddsförordningen GDPR, EU 2016/679

Information som ska arkiveras
En viktig uppgift med många kopplingar till informationssäkerhet är att säkra riktigheten hos och skapa tillgänglighet till allmänna handlingar över tid.

Arkivering ställer särskilda krav, särskilt när det gäller elektronisk information. Riksarkivet utfärdar föreskrifter på området.

- Arkivlag (1990:782)
- Arkivförordning (1991:446)
- Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1).
- Riksarkivets föreskrifter om och allmänna råd om tekniska krav på
- elektroniska handlingar (RA-FS 2009:2).

Rättsliga krav på informationssäkerhet i samhällsviktiga tjänster
EU:s NIS-direktiv ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Direktivet har införlivats i den svenska lagstiftningen genom:

- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)
- Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1175).

Rättsliga krav inom elektronisk kommunikation
Lagen om elektronisk kommunikation reglerar hur information ska hanteras i elektroniska medier och vänder sig främst till telekommunikationsoperatörer. Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet.

- Lag (2003:389) om elektronisk kommunikation
- Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid (PTSFS 2007:2)

Informationssäkerhet inom hälso- och sjukvård
Inom hälso- och sjukvården hanteras stora mängder information som är känslig ur integritetssynpunkt. Det är därför av stor vikt att informationshanteringen inom hälso- och sjukvården är organiserad så att den tillgodoser patientsäkerhet och god kvalitet.

- Patientdatalag (2008:355)
- Patientdataförordning (2008:360)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

It-relaterad brottslighet
Rättslig reglering bidrar till ökad informationssäkerhet genom krav på att åtgärder vidtas men även genom att kriminalisera vissa handlingar. Många brott, exempelvis bedrägeri, begås i

dag ofta med hjälp av informationsteknik. Ett brott med uttrycklig koppling till it är dataintrång.

- Brottsbalk (1962:700)

Övriga informationssäkerhetsrelaterade föreskrifter och förordningar

- Förordning (2006:637) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
- MSB:s föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7)
- MSB:s föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter (MSBFS 2020:8)
- MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1).
- MSB:s föreskrifter och allmänna råd om kommuners risk- och sårbarhetanalyser (MSBFS 2020:6)
- MSB:s föreskrifter om civila myndigheters kryptoberedskap (MSBFS 2009:11)

7.2.4 Figur- och tabellförteckning

Figur **Sid**