Riktlinjer för informationssäkerhet inom Stockholms läns landsting

Innehållsförteckning

1 Introduktion till informationssäkerhet

1.1 Allmänt

Stockholm läns landstings verksamhet är omfattande och komplex, med många olika intressenter och med ett stort beroende av information. Information är ett vitt begrepp som inkluderar allt från kunskap och information som enskilda medarbetare besitter, till information lagrad i IT-system.

En effektiv och säker användning av information är en förutsättning för landstingets verksamhet och för förtroendet för dess förmåga att leverera service till medborgarna. Offentlighetsprincipen ställer ytterligare krav på landstingets informationshantering, liksom speciella lagar inom verksamhetsområden som hälso- och sjukvård och trafik. Detta sammantaget gör information till en av landstingets viktigaste resurser.

Informationssäkerhet är därför viktigt för landstinget och informationssäkerhetsarbetet berör alla delar av landstingets verksamhet.

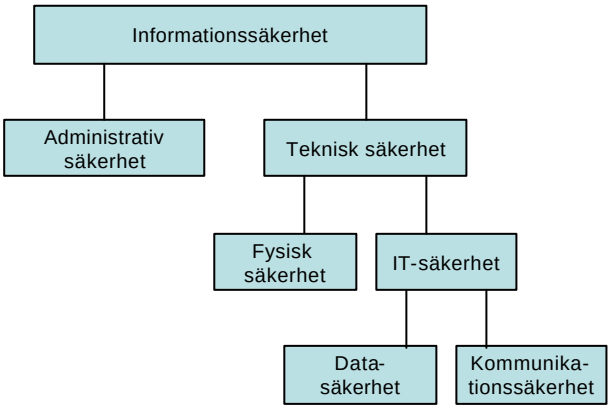
Ett sunt och vaket säkerhetsmedvetande hos alla berörda är en förutsättning för ett väl fungerande informationssäkerhetsarbete.

1.2 Vad är informationssäkerhet?

Informationssäkerhet är att säkerställa att information i alla dess former, som skriftlig, muntlig och elektronisk, finns tillgänglig när den behövs, att den är korrekt, att obehöriga inte kan få tillgång till den och att händelser i informationsbehandlingen kan spåras.

Informationssäkerhetsarbetet är omfattande och kräver ofta uppdelning i olika områden, för att kunna angripas på ett rationellt och effektivt sätt. Det kräver många olika kompetenser och engagemang från ledning, systemägare, användare, administrativ personal, IT-personal m.fl.

Informationssäkerhet kan delas upp i två huvudområden, administrativ respektive teknisk säkerhet, vilket illustreras i nedanstående bild.



1.2.1 Administrativ säkerhet

Administrativ säkerhet innefattar skyddsåtgärder av administrativ art, dvs. hur styrning och uppföljning av informationssäkerheten ska ske, hur ansvar för informationssäkerheten ska fördelas, hur åtkomst till informationen ska regleras, hur rutinerna ska utformas och hur arbetsmomenten ska utföras.

Dessa riktlinjer är en del av den administrativa säkerheten.

1.2.2 Fysisk säkerhet

Den fysiska säkerheten för information syftar till att skydda mot obehörigt tillträde och åtkomst, skador och störningar.

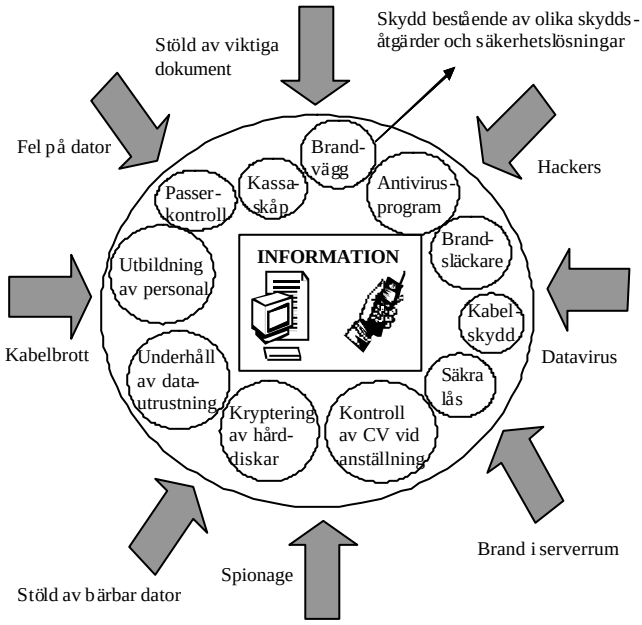
1.2.3 IT-säkerhet

Information bearbetas, lagras och överförs ofta via IT-system och nätverk. Därför innefattar informationssäkerhet även IT-säkerhet, vilket inkluderar åtgärder för skydd av IT-system och deras data, vid databehandling och data- och telekommunikation.

1.3 Skyddsåtgärder

Landstingets samtliga verksamheter måste vidta skyddsåtgärder, med syfte att uppnå och vidmakthålla eftersträvad nivå på informationssäkerheten. Med skyddsåtgärder avses i detta sammanhang alla de administrativa och tekniska åtgärder som vidtas för att skydda informationen.

Nedanstående bild visar exempel på olika typer av tänkbara hot och skyddsåtgärder.



För att bestämma vilka skyddsåtgärder som behövs måste de hot som information kan utsättas för vara kända. Det är viktigt att beakta att hotbilden kan förändras när information byter bärare, t.ex. när elektronisk information skrivs ut på papper eller förmedlas via telefon.

De skyddsåtgärder som väljs ska stå i proportion till de olika risker som respektive organisation kan utsättas för. Valet av skyddsåtgärder är beroende av resultatet från genomförda riskanalyser, samt värdet på det som ska skyddas satt i relation till kostnaden för att införa och upprätthålla föreslagna skyddsåtgärder.

Alla skyddsåtgärder ska dokumenteras på ett sådant sätt att möjligheter ges att kontrollera att eftersträvad skyddsnivå uppnås.

1.4 Mål

Landstingets informationssäkerhetspolicy definierar fyra skyddsområden för informationen: *Tillgänglighet, Konfidentialitet, Riktighet och Spårbarhet.*

Målet för landstingets informationssäkerhetsarbete är att, genom att införa och upprätthålla skydd på lämpliga nivåer inom ovanstående skyddsområden, möjliggöra för landstingets verksamheter att uppnå sina mål.

1.5 Syfte och omfattning

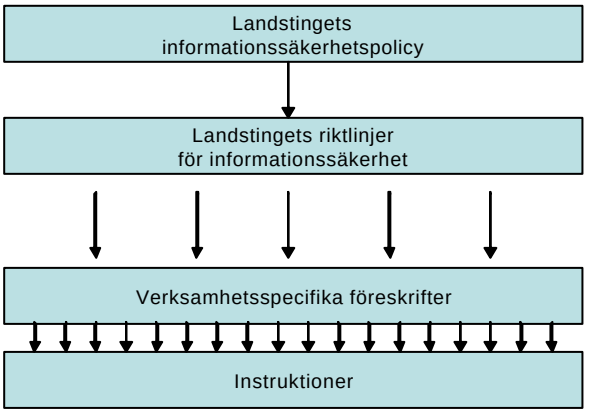
Syftet med detta dokument är att ge riktlinjer och vägledning för informationssäkerheten och -säkerhetsarbetet inom landstinget. Dessa riktlinjer, vilka är en konkretisering av landstingets informationssäkerhetspolicy, är styrande för landstingets informationshantering, och ska efterlevas av samtliga förvaltningar och bolag inom landstinget och, genom avtal, av samtliga som arbetar på uppdrag av landstinget.

Den som ingår avtal med extern part, som leder till informationsanvändning eller -utbyte, ansvarar för att risker relaterade till detta analyseras, att kraven på informationssäkerhet specificeras i avtalet och att uppföljning av avtalad skyddsnivå sker.

För att uppnå målet med informationssäkerheten ska säkerhetsarbetet omfatta samtliga områden behandlade i dessa riktlinjer.

1.6 Regelverk för informationssäkerhet

Landstingets regelverk för informationssäkerhet är uppbyggd enligt följande struktur:



Informationssäkerhetspolicyn beskriver landstingets syn på informationssäkerhet och de övergripande principer som gäller för informationssäkerheten. Informationssäkerhetspolicyn antas av landstingsfullmäktige.

Riktlinjer för informationssäkerhet konkretiserar informationssäkerhetspolicyn och ger riktlinjer avseende skyddsåtgärder och -nivåer. Riktlinjerna är framtagna med stöd av standarden för informationssäkerhet, SS-ISO/IEC 17799, och avser inte att i detalj beskriva hur skyddsåtgärderna ska utformas. Riktlinjerna antas av landstingsstyrelsen.

Varje nämnd och styrelse, ska anta *föreskrifter* som innehåller preciseringar och tillägg till policy och riktlinjer, med utgångspunkt från den egna organisationens specifika behov.

Med utgångspunkt från föreskrifterna, ska vid behov *instruktioner* fastställas av respektive förvaltning och bolag, som detaljerat beskriver hur rutiner och skyddsåtgärder ska utformas och tillämpas, för att informationssäkerheten ska kunna realiseras.

2 Informationssäkerhetsorganisation

2.1 Allmänt

Detta kapitel beskriver riktlinjer för hur roller och ansvar ska fördelas samt hur informations-säkerhetsarbetet ska organiseras.

För att uppnå och bibehålla god informationssäkerhet, krävs fördelning av roller och ansvar liksom samordning och uppföljning av informationssäkerhetsarbetet. Genom detta skapas en tydlig organisation och därmed förutsättningar för effektiva rutiner.

Vid utredningar om organisationsförändringar, där verksamhetsansvar förs över till annan förvaltning, till bolag eller annan juridisk person, måste analyser genomföras, dels av de rättsliga förutsättningarna för överförandet av information och system, dels av hur roller och ansvar ska överföras.

2.2 Övergripande informationssäkerhetsansvar

2.2.1 Landstingsfullmäktige

Landstingsfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för landstinget.

2.2.2 Landstingsstyrelsen

Landstingsstyrelsen ansvarar, enligt sitt reglemente, för att landstingets informationssäkerhets-policy och riktlinjer för informationssäkerheten utformas och hålls aktuella. Landstingsstyrelsen har ansvaret för samordning och uppföljning av informationssäkerheten och har därmed det övergripande ansvaret för informationssäkerheten inom landstinget.

2.2.3 Landstingsdirektören

Landstingsdirektören har landstingstingsstyrelsens uppdrag att tillse att informationssäkerhets-arbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser, så att informationssäkerhetsmålet kan uppnås.

I landstingsdirektörens uppdrag ingår även, att i samråd med berörda förvaltningar och bolag, utforma handlingsplaner för informationssäkerhetsarbetet inom landstinget och tillse att dessa beaktas i förvaltningars och bolags årliga budgetförslag.

Landstingsdirektören ska utse en informationssäkerhetschef med ansvar för samordning av informationssäkerhetsarbetet inom landstinget.

2.2.4 Informationssäkerhetschefen

Informationssäkerhetschefen verkställer samordningen av informationssäkerhetsarbetet inom landstinget och förvaltar landstingets informationssäkerhetspolicy och dessa riktlinjer. Dessutom ska denne

- bistå förvaltningschef och motsvarande med råd och rekommendationer i samverkan med lokala informationssäkerhetssamordnare,

- inhämta uppgifter om informationssäkerhetsläget i landstinget som ett led i uppföljningen av informationssäkerheten,
- rapportera iakttagelser och föreslå åtgärder av övergripande principiell karaktär,
- vara landstingets representant i kontakter med externa organisationer inom informationssäkerhetsområdet,
- vara remissinstans i frågor som rör informationssäkerhet,
- genom aktiv omvärldsbevakning följa och påverka utvecklingen inom informationssäkerhetsområdet.

2.2.5 Landstingsrevisorerna

Landstingsrevisorernas uppgift är att granska den interna kontrollen, vilket här innefattar att granska om ledning och styrning, uppföljning och kontroll av informationssäkerheten är tillfredställande.

2.3 Roller och ansvar i verksamheten

I enlighet med vad som gäller för övrig verksamhet inom landstinget, är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten i denna verksamhet.

Nedan beskrivs informationssäkerhetsansvar för vissa generella roller. Beroende på lokala förhållanden, kan även andra roller behöva beskrivas och ansvar fastställas.

2.3.1 Styrelser och nämnder

Varje nämnd och styrelse är ytterst ansvarig för informationssäkerheten inom sin förvaltning respektive bolag. De ska därför anta egna föreskrifter för informationssäkerheten, i enlighet med informationssäkerhetspolicyn och dessa riktlinjer. Det åligger också varje nämnd och styrelse att avsätta medel för informationssäkerhetsarbetet, årligen planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Nämnd och styrelse är personuppgiftsansvarig inom sin organisation, enligt personuppgiftslagen (PuL). Personuppgiftsansvarig ska utse ett eller flera personuppgiftsombud.

I de fall personuppgifter hanteras på uppdrag utanför den egna organisationen, ska avtal om personuppgiftsbiträde upprättas, i enlighet med PuL.

2.3.2 Personuppgiftsombud

Personuppgiftsombud har till uppgift att tillse att personuppgifter behandlas på ett lagligt och korrekt sätt. Personuppgiftsombudet ska bl.a. påpeka eventuella brister i behandlingen. Ombudet ska anmäla missförhållanden, som efter påpekande inte åtgärdas, till Datainspektionen, som är tillsynsmyndighet när det gäller behandling av personuppgifter.

Personuppgiftsombudet ska föra en förteckning över de behandlingar, som skulle ha omfattats av anmälningsskyldighet, om ombudet inte funnits.

2.3.3 Förvaltningschef/VD

Förvaltningschef/VD har, inom sin verksamhet, ansvaret för att utforma och kommunicera föreskrifter, verkställa och följa upp styrelse respektive nämnds beslut och att åtminstone årligen rapportera status på informationssäkerheten till nämnd respektive styrelse.

I ansvaret ingår även att säkerställa att all informationshantering sker i enlighet med informationssäkerhetspolicy, riktlinjer och föreskrifter, och att, där så krävs, fastställa instruktioner. Denne ansvarar även för att kontinuitetsplaner utarbetas för respektive verksamhet.

Alla viktiga tillgångar inom landstinget ska redovisas. Förvaltningschef/VD ansvarar för att förteckning över alla viktiga tillgångar förs. Det åligger även denne att säkerställa att ägare för dessa tillgångar utses, med ansvar för att vidta nödvändiga skyddsåtgärder.

Informationssäkerhet är en naturlig del av chefsansvaret och är kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som får ett delegerat verksamhetsansvar, också ansvarar för informationssäkerheten inom den verksamheten.

Förvaltningschef/VD ska utse en informationssäkerhetssamordnare, med ansvar för att koordinera arbetet med informationssäkerhet inom den egna organisationen.

2.3.4 Informationssäkerhetssamordnare

Inom varje förvaltning och bolag ska utses en informationssäkerhetssamordnare. Denne rapporterar direkt till förvaltningschef/VD och ansvarar för följande:

- Utforma förslag till föreskrifter för informationssäkerheten.
- Sprida kunskap om regler, metoder och tekniker avseende informationssäkerheten.
- Samordna det för organisationen och verksamheten gemensamma informationssäkerhetsarbetet.
- Koordinera arbetet med incidenthantering och riskanalyser.
- Följa upp efterlevnaden av policy, riktlinjer, föreskrifter och instruktioner.
- Vara kontaktperson mot landstingets informationssäkerhetschef.

2.3.5 Informationsägare

För varje viktig informationstillgång ska utses en informationsägare, med uppdrag att hantera alla delar av informationssäkerheten, vilket inkluderar klassificering av informationen.

Informationsägaren ansvarar för att beslut fattas om användares åtkomsträttigheter och att dessa överensstämmer med deras behörigheter. Dessutom ansvarar denne för att riskanalyser genomförs och att samordning av riskanalyser sker med andra informationsägare.

När information hanteras i IT-system ska informationsägarens krav ligga till grund för systemägarens val av skyddsåtgärder.

Informationsägarskapet växlar när information överlämnas från en organisation till en annan. Det ankommer på respektive informationsägare som överlämnar information, att ställa krav på hur mottagaren ska hantera informationen, med syfte att säkerställa informationssäkerheten i informationsbehandlingskedjan.

Vid behov kan det för en verksamhetskritisk process utses en informationsägare, med uppdrag att säkerställa att informationssäkerheten beaktas i hela processen.

2.3.6 Systemägare

För varje IT-system och nätverk ska det utses en systemägare, med uppdrag att hantera informationssäkerheten rörande sitt system.

Systemägaren ska besluta om nyutveckling, vidareutveckling och avveckling, samt vid behov utse systemförvaltare, som ges uppdraget att inom givna ekonomiska ramar ta det funktionella ansvaret för systemet.

Systemägaren, som i allmänhet är chefen för den organisatoriska enhet som har huvudintresset i ett informationssystem, ska tillse

- att skyddsnivån för systemet specificeras, genom att utforma instruktioner, utifrån fastlagda föreskrifter och informationsägarnas krav,
- att fastställd modell för förvaltning av system efterlevs och att det upprättas system-specifika förvaltningsplaner,
- att avbrottsplaner för systemet utarbetas,
- att användarna informeras om vilken skyddsnivå som gäller för systemet och vilka krav som därmed ställs på dessa,
- att rutin för rapportering och uppföljning av informationssäkerhetsincidenter, funktionsfel och brister utvecklas,
- att incidenter, funktionsfel och brister analyseras och hanteras,
- att instruktioner för beviljande och kontroll av rättigheter till systemet utformas,
- att rutiner för uppföljning av avvikelser eller försök till avvikelser mot åtkomstreglerna utarbetas,
- att användarna tilldelas rättigheter i enlighet med informationsägarnas beslut,
- att förteckning över användare och rättigheter förs och att regelbundet följa upp dessa,
- att krav på informationssäkerhet och funktionalitet beaktas i samband med anskaffning och utveckling av informationssystem,
- att åtgärder vidtas för att hantera identifierade risker utifrån genomförda riskanalyser,
- att systemdokumentation upprättas och hålls uppdaterad,
- att användarna ges adekvat utbildning.

2.3.7 IT-chef/samordnare

I varje organisation där det har utsetts en IT-chef/samordnare, ska denne

- införa och upprätthålla informationssäkerheten för de IT-system, den information och den utrustning man givits i uppdrag att hantera, i enlighet med gällande regelverk,
- utforma instruktioner för IT-verksamheten baserade på dessa riktlinjer och fastställda föreskrifter,
- tillse att IT-personalen följer gällande regler för informationssäkerheten,
- ansvara för att IT-personalen får den utbildning i informationssäkerhet som krävs,
- avtala om och fortlöpande kontrollera att anlitade leverantörer inom IT-området uppfyller kraven på informationssäkerhet.

2.3.8 Informationsanvändare

Informationsanvändare är samtliga personer som i sin yrkesutövning hanterar information inom landstinget, vilket inkluderar såväl anställda som andra användare.

Informationsanvändarnas medverkan är väsentlig för en effektiv informationssäkerhet. De ska göras medvetna om sin skyldighet att följa uppställda informationssäkerhetsregler liksom att rapportera informationssäkerhetsincidenter, funktionsfel och brister, enligt fastställda rutiner.

Varje informationsanvändare som skapar en ny informationsmängd, är skyldig att tillse att denna inkluderas i förteckningen över tillgångar i respektive förvaltning och bolag.

2.4 Samordning och uppföljning

För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ges informationssäkerhetschefen möjlighet att inrätta ett informationssäkerhetskollegium. Kollegiet ska bestå av informationssäkerhetssamordnare i förvaltningar och bolag.

3 Hantering av tillgångar och risker

3.1 Allmänt

Detta kapitel beskriver riktlinjer för riskhantering, dvs. processen som styr att risker kontinuerligt bedöms och tas om hand med lämpliga skyddsåtgärder.

Viktiga komponenter i riskhanteringen är registrering och klassificering av information samt genomförande av riskanalyser. Riskanalys, som innebär att utifrån hotbilder identifiera och bedöma risker, är ett centralt område inom landstingets informationssäkerhetsarbete. Analyserna ska utmynna i att lämpliga åtgärder vidtas för att hantera de identifierade riskerna.

Korrekt hantering, klassificering och märkning av tillgångarna, är viktiga förutsättningar för informationssäkerhetsarbetet, såväl i det dagliga arbetet, som när det gäller strategiska beslut rörande tillgångarna.

3.2 Hantering av tillgångar

Information och andra tillgångar ska hanteras enligt de rutiner och klassificeras och märkas med hjälp av de system, som fastställs av respektive förvaltning och bolag. Med hantering avses t.ex. lagring och kopiering, överföring via post, fax, e-post och tal samt arkivering och förstöring.

3.2.1 Förteckningar

Det ska finnas en förteckning över viktiga tillgångar inom respektive förvaltning och bolag. Följande tillgångar ska finnas med i förteckningen:

- Programvaror.
- Informationstillgångar, som databaser, datafiler och dokumentation.
- Fysiska tillgångar.
- Nyckelpersoner.
- Avtal.
- Immateriella tillgångar, som patent och varumärken.

Personuppgiftslagen och vårdregisterlagen ställer härutöver legala krav på förteckningar och register inom landstinget.

3.2.2 Klassificering

Alla viktiga informationstillgångar och IT-system inom landstinget ska klassificeras, för att klarlägga hur stor tillgångens betydelse är. Det är viktigt att klassificeringen sker med omsorg och förnuft, då den ska fungera som underlag för riskanalyser och göra det möjligt att prioritera risker och skyddsåtgärder. Klassificeringen av respektive tillgång måste omprövas regelbundet, som ett naturligt inslag i det kontinuerliga säkerhetsarbetet.

Rutiner för klassificering ska fastställas, där kraven på tillgänglighet, riktighet och konfidentialitet ska vara utgångspunkten. Klassificeringen av en tillgång sker med utgångspunkt i att information och informationsbehandling är skyddsvärda resurser för den aktuella verksamheten. Tillgången tilldelas sedan en informationsklass som motsvarar dess betydelse.

Nedanstående matris, som är en klassificeringsmodell framtagen av Statskontoret och anpassad för landstinget, är den modell som bör användas inom landstinget. Nivåbestämningen utgår från bedömd skada vid obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång eller IT-system. Nivå 1 innebär ingen eller ringa skada och nivå 3 innebär allvarlig skada.

N	Konfidentialitet	Riktighet	Tillgänglighet
3	Informationstillgång som innehåller känslig information som om den kommer i orätta händer kan medföra **allvarlig skada**. Generellt tillämpligt: 1. Informationstillgång som är eller kan bli föremål för sekretess enligt sekretesslagen. 2. Informationstillgång som kan bli föremål för tillämpningskrav enligt särskild lagstiftning inom respektive verksamhetsområde (t.ex. patientjournallagen). 3. Informationstillgång rörande skyddad identitet. *(Sekretesslagen 2:1 och 2:2 förhållande till främmande makt och krav på försvarssekretess omfattas ej).*	Oriktig information kan medföra **allvarlig skada**. Generellt tillämpligt: 1. Informationstillgång med särskilt höga krav på riktighet. T.ex. där personligt ansvar uppenbart kan utkrävas vid felaktigheter. (Ekonomiadministrativa system, behandling av personuppgifter etc.) 2. IT-system eller informationstillgång för kritiska processer i verksamheten.	IT-system eller informationstillgång som ingår i eller stöder kontinuerlig verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå i produktionen med alternativa metoder och procedurer. Avbrott kan medföra **allvarlig skada**. Generellt tillämpligt: 1. För verksamheten mycket kritiska IT-system eller informationstillgångar. 2. E-tjänster mot allmänhet och andra intressenter med krav på mycket hög servicenivå.
2	Informationstillgång som innehåller känslig information som om den kommer i orätta händer kan medföra **skada**. Generellt tillämpligt för: 1. Information där utlämnande skall föregås av sekretessprövning 2. Personuppgifter i allmänhet eller som enligt PuL är att betrakta som känsliga. 3. Information som kan bli föremål för sekretess. 4. Information som styrs av verksamhetsspecifik lagstiftning. 5. Uppgifter av intern karaktär vilka, utan andra restriktioner, endast egen personal bör ha tillgång till.	Oriktig information kan medföra **skada**. Generellt tillämpligt: 1. Informationstillgång som omfattas av lagrum där riktighetskrav anges (t.ex PuL, eller speciallagstiftning). 2. IT-system eller informationstillgång som ingår i myndighetsutövning. 3. Information eller IT-system där krav på spårbarhet eller oavvislighet föreligger.	IT-system eller informationstillgång som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada**. Generellt tillämpligt: 3. IT-system eller informationstillgång som ingår i eller utgör stöd för myndighetsutövning och/eller kärnverksamhet. 4. E-tjänster mot allmänhet och andra intressenter.
1	Informationstillgång som endast innehåller information som är offentlig allmän uppgift eller information som om den kommer obehöriga till del medför **ingen skada**. Information som är avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser.	Oriktig information kan endast medföra **ringa eller ingen skada**.	IT-system eller informationstillgång där verksamhetsberoendet är lågt och avbrott endast kan medföra **ringa eller ingen skada**.

3.2.3 Märkning

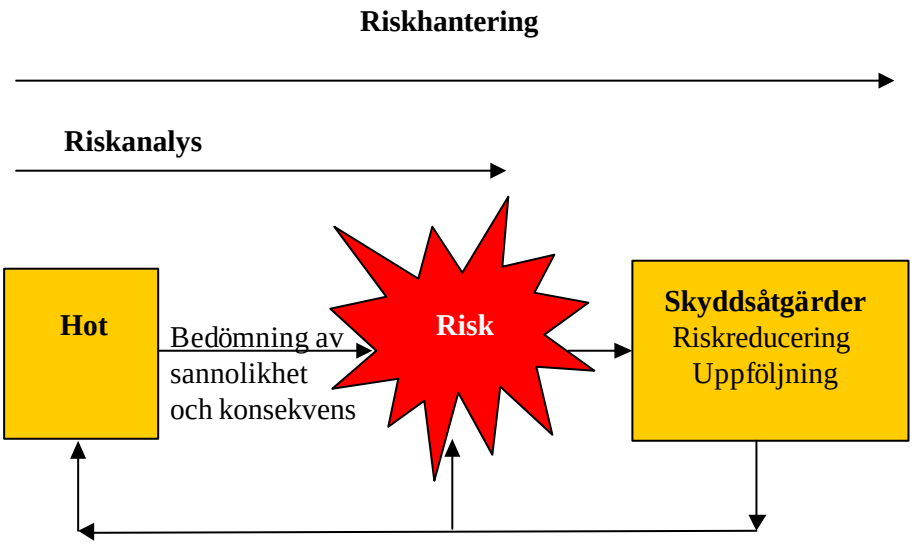
Märkning av information ska ske enligt det klassificeringssystem som har fastställts inom respektive förvaltning eller bolag. Detta ska gälla för information i såväl fysisk som elektronisk form.

När information, som klassificeras som hemlig enligt sekretesslagen, genereras i form av utskrifter, skärmbilder, e-post eller filöverföringar, ska klassificeringen tydligt framgå. Om det går att märka informationen med fysiska etiketter ska detta ske. Går inte det bör informationen istället märkas elektroniskt.

3.3 Riskanalys

Riskanalyser stödjer verksamhetens säkerhetsarbete och används som ett verktyg för att analysera risker utifrån potentiella hot. Riskerna bedöms utifrån hur stor sannolikheten är att hoten realiseras och konsekvenserna av detta. Riskanalyserna ger underlag för att fastställa de skyddsåtgärder som behöver finnas och ska utmynna i prioriterade åtgärdsplaner för att hantera riskerna.

Bilden nedan beskriver processen för riskhantering och riskanalysens roll, samt visar hur risker kan reduceras/elimineras med hjälp av skyddsåtgärder.



Åtgärdsplanerna ska vara balanserade, dvs. de skyddsåtgärder som väljs ska stå i proportion till de risker som varje verksamhet är utsatt för.

Riskhantering ska vara en kontinuerlig process och riskanalyser bör genomföras i samband med förändringar i verksamheten, processerna och informationssystemen eller motsvarande.

3.4 Hantering av informationssäkerhetsincidenter

Inom varje förvaltning och bolag ska fastställas rutiner för rapportering och uppföljning av säkerhetsincidenter rörande informationssäkerheten.

Med säkerhetsincident avses en händelse där någon aspekt av informationssäkerheten hotas t.ex. brott mot sekretess, integritetsförlust avseende information eller IT-system, driftavbrott eller förhindrande av tillgång till information.

4 Åtkomst till information

4.1 Allmänt

Detta kapitel beskriver riktlinjer för att styra informationsanvändares åtkomst till information och för att förhindra obehörig åtkomst.

Åtkomst till information ska regleras av informationsägare.

4.2 Styrning av åtkomst till elektronisk information

All tillgång till elektronisk information inom landstinget, ska styras med hjälp av följande administrativa och tekniska skyddsåtgärder:

SKYDDSÅTGÄRD	SYFTE
Åtkomstadministration	För att säkerställa att endast behöriga informationsanvändare har tillgång till viss information ska åtkomsträttigheten godkännas innan den delas ut. Rättigheten ska vid varje tillfälle baseras på användarens aktuella behörighet, utifrån arbetsuppgifter och organisatorisk tillhörighet.
Åtkomstkontroll	Tillgång till alla IT-system ska styras med hjälp av åtkomstkontroll. Varje användare ska autenticeras, dvs. identiteten ska verifieras, vid inloggning.
Loggning och uppföljning	För att säkerställa att endast behöriga användare har åtkomst till viss information, ska åtkomst loggas och tilldelade rättigheter följas upp.

4.2.1 Åtkomstadministration

Det ska fastställas rutiner för hur beställning, registrering, ändring och avregistrering av rättigheter ska göras.

Granskning och uppföljning av användarnas åtkomsträttigheter ska göras regelbundet och efter varje större organisations- eller systemförändring.

Åtkomst med utvidgade rättigheter, s.k. administratörsrättigheter, som möjliggör för användaren att t.ex. ändra rättigheter eller konfigurationer i applikationer, databaser, operativsystem eller nätverk, ska begränsas till så få personer som möjligt.

Systemadministrativa arbetsuppgifter ska alltid vara kopplade till personliga användaridentiteter, för att säkerställa spårbarhet avseende genomförda aktiviteter. För administratörer med omfattande behörigheter, där ovanstående inte kan tillämpas, ska särskilda skyddsåtgärder vidtas, t.ex. upprättande av manuell åtkomstlogg.

4.2.2 Åtkomstkontroll

En av de, ur säkerhetssynpunkt, viktigaste aspekterna på åtkomstkontroll är att man säkert vet vem som är vem i IT-systemen. Detta sker genom autenticering, dvs. verifiering av användarens identitet. Alla användare ska därför ha en unik identitet.

Det grundläggande kravet på utformningen av identiteter är att namnsättningen är standardiserad, så att användaridentiteten kan härledas till den verkliga personen.

Användaridentiteten är personlig och får inte lånas ut.

Användaridentitet i kombination med lösenord ska användas för att säkerställa att användare av IT-system är behöriga.

Lösenorden ska konstrueras så att de blir svåra att röja med hjälp av t.ex. automatiserad lösenordsprovare.

Lösenord ska vara hemliga och ska bytas regelbundet.

Vid hantering av information, klassificerad enligt klassificeringsmodellen i någon av klasserna K3 eller R3, bör stark autenticering, dvs. autenticering med hjälp av en kryptografisk algoritm och tillhörande hemlig nyckel, användas.

4.2.3 Övervakning, loggning och uppföljning

Loggning ska ske på samtliga verksamhetskritiska IT-system, så att det i efterhand går att följa enskilda användares aktiviteter.

Loggarna ska vara skyddade mot obehörig åtkomst och manipulation. Loggarna ska omfattas av fastställda rutiner för säkerhetskopiering och arkivering.

För att säkerställa logginformationens värde, ska rutiner fastställas för synkronisering av loggade IT-systems systemklockor.

Samtliga loggar ska granskas regelbundet enligt fastställd rutin, där det ska framgå vad som ska loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Vidare ska beslut finnas för hur överträdelser ska hanteras.

Periodiciteten för granskning av loggarna ska vara minst var fjärde månad.

4.3 Extern informationsanvändning

För informationsanvändare som ges tillgång till landstingets information från miljöer utanför landstingets kontroll, ska särskilda krav ställas på autenticering av användare och utrustning, liksom på kryptering.

4.4 Automatisk utloggning

För att förhindra obehörig åtkomst till IT-system, bör användaren inte lämna arbetsstationen påloggad. Det ska finnas en funktion som säkerställer automatisk utloggning ur systemet eller aktivering av lösenordsskyddad skärmsläckare efter en viss tids inaktivitet.

4.5 Styrning av åtkomst till övrig information

Skriftlig information ska omgärdas av skyddsåtgärder vid all hantering, dvs. kopiering, distribution, förändring, läsning, makulering, förvaring och arkivering.

När information förvaras i säkra utrymmen, för att den är högt klassificerad enligt klassificeringsmodellen, ska en förteckning föras över de personer som har åtkomsträttigheter till det säkra utrymmet.

Ljud- och videoupptagningar ska hanteras i enlighet med gällande författningar och lämpliga skyddsåtgärder ska införas, som förhindrar obehörig åtkomst eller manipulation och oavsiktlig förstöring.

Utformningen av skyddsåtgärder när information byter bärare, t.ex. när elektronisk information skrivs ut på papper eller förmedlas via telefon, måste anpassas. När information överförs muntligt bör den som förmedlar informationen förvissa sig om att mottagaren är den avsedda, och att lämpliga skyddsåtgärder mot olika typer av överhöring har vidtagits.

När information överlämnas, ska mottagaren informeras om hur informationen ska hanteras och förvaras.

5 Driftsäkerhet

5.1 Allmänt

Detta kapitel beskriver riktlinjer för drift och underhåll av IT-system, med syfte att säkerställa verksamhetens krav på informationssäkerhet. IT-system inkluderar nätverk och system för data- och telekommunikation.

5.2 Säkerhetskrav på systemmiljön

Landstinget ska ha en systemmiljö med åtskilda produktions-, utvecklings- och testmiljöer. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för utvecklings- och testmiljöerna.

5.3 Systemförvaltning

För att upprätthålla säker och tillförlitlig tillgång till information, ska administration, drift och underhåll av IT-system ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning.

Samtliga system ska ha fastställda rutiner för administration, drift och underhåll, manifesterade i ett systemförvaltningsavtal. Avtalen ska säkerställa att systemen hanteras på ett enhetligt och informationssäkerhetsmässigt korrekt sätt och att beroendet av enskilda personers kunskap minskas.

5.3.1 Säkerhetsuppdateringar

Leverantörernas säkerhetsuppdateringar ska installeras fortlöpande. För att säkerställa att driften inte påverkas negativt, ska säkerhetsuppdateringarna kontrolleras och analyseras innan de installeras i produktionsmiljön.

5.3.2 Styrning av ändringar

Samtliga ändringar, som utförs i IT-system, ska noggrant planeras och en analys av eventuella konsekvenser göras.

Ändringar, som bedöms kunna påverka informationssäkerheten, ska testas i separat testmiljö innan de införs i produktionsmiljön.

Rutiner ska fastställas för ändringshantering och testning, vilka ska vara kända av berörda personer. Rutinerna ska även säkerställer att det är möjligt att återgå till läget före ändringen.

5.3.3 Felhantering

Allvarlig störning i produktionsmiljön kräver ofta att åtgärder genomförs omgående, s.k. felhantering, där de fastställda rutinerna för ändringshantering inte kan följas. Sådana akuta ändringar ska dokumenteras och i efterhand följas upp enligt rutinen för ändringshantering.

5.3.4 Kapacitetsplanering

Kapacitetsplanering syftar till att förutse kapacitets- eller prestandaproblem. Regelbunden mätning och uppföljning av kapaciteten ska genomföras. Detta är särskilt viktigt för de system som bedöms som verksamhetskritiska.

5.4 Skydd mot datavirus

All utrustning, som kan drabbas av datavirus eller annan skadlig kod, ska skyddas. Viruskontroll ska ske obligatoriskt och automatiskt. Virusdefinitionsfiler ska automatiskt uppdateras löpande, för att garantera likartat och aktuellt skydd.

Det ska fastställas föreskrifter och instruktioner för hantering av virusskydd och -incidenter, vilka ska innefatta instruktioner för hur användare ska identifiera, åtgärda och rapportera möjliga virusangrepp.

Generellt ska vaksamhet och restriktivitet iakttas när det gäller t.ex. bifogade filer i e-post, användning av disketter respektive nedladdning av filer och program från Internet.

5.5 Användning av arbetsstationer, bärbara datorer och övrig utrustning

Alla arbetsstationer, bärbara datorer och övrig utrustning, t.ex. handdator, som ansluts till något av landstingets nätverk eller till nätverksansluten utrustning, ska skyddas enligt instruktioner som fastställs inom respektive förvaltning och bolag, och vara konfigurerade enligt lokalt definierade standardkonfigurationer.

Dessa standardkonfigurationer ska också ge användaren möjlighet att lagra information på gemensamma lagringsmedia.

Modem och annan utrustning för fjärrkommunikation får inte anslutas till landstingets nätverk eller till nätverksansluten utrustning, utan att säkerhetsaspekterna utretts och nödvändiga skyddsåtgärder vidtagits.

Information, klassificerad enligt klassificeringsmodellen i klassen K3, som inte lagras på media i säkra utrymmen, ska krypteras.

Landstingets utrustning är avsedd att användas för arbetsrelaterade ändamål.

5.6 Säkerhetskopiering och återläsning av data

Säkerhetskopiering av information och programvara ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhets- respektive legala krav, enligt fastställd instruktion.

Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.

Säkerhetskopior och original ska förvaras på skilda platser och med skyddsåtgärder som överensstämmer med informationens klassificering.

5.7 Drift hos extern part

Vid anlitande av en extern part för drift och underhåll av IT-system, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi. Kraven på informationssäkerhet ska regleras i avtalet mellan parterna. Uppföljning av avtalad säkerhetsnivå ska ske.

Risker som följer av beroendet av en viss leverantör ska minimeras och åtgärder vidtas, som kan hantera konsekvenserna av att en leverantör inte kan fullfölja sitt uppdrag.

5.8 Systemdokumentation

Det ska finnas systemdokumentation för varje IT-system. Dokumentationen ska normalt bestå av system-, drifts- och användardokumentation.

Dokumentationen ska vara fullständig och aktuell. Ändringar av dokumentationen ska ske enligt fastställda rutiner. Rutinen ska även omfatta kopior av dokumentationen.

Det ska finnas en kopia av systemdokumentation, och andra för systemets användning och drift viktiga dokument, förvarad skild från originalet.

Arkivering av systemdokumentation ska ske i enlighet med landstingets bestämmelser och legala krav.

Delar av systemdokumentationen kan innehålla känslig information, t.ex. om systemets säkerhetsfunktioner, och ska därför förvaras så att den endast är åtkomlig för behörig personal.

5.9 Illegal kopiering och användning

Upphovsrätten ska respekteras. Installation, användning, kopiering och vidarebefordran av programvara eller datafiler, inklusive ljud och bild, är inte tillåten utan tillstånd eller licens.

6 Kommunikations- och nätverkssäkerhet

6.1 Allmänt

Detta kapitel beskriver riktlinjer för kommunikations- och nätverkssäkerhet i landstingets olika nätverk, med syfte att minska risken för obehörig åtkomst respektive brister i tillgängligheten till information, och gäller för samtliga förvaltningar och bolag, samt de externa verksamheter som nyttjar landstingets nätverk.

Riktlinjerna inkluderar även anslutningar till externa och publika nätverk, såsom Internet.

6.2 Säkerhetskrav på nätverksmiljön

Landstingets olika nätverk ska vara logiskt separerade. Varje nätverk ska utformas så att det finns definierade gränssnitt, såväl fysiskt som logiskt, mot andra nätverk. ´

Respektive nätverk bör dessutom vara logisk separerade i s.k. nätverkssegment. Denna separering minskar risken för obehörig åtkomst samt möjliggör uppdelning i åtskilda produktions-, utvecklings- och testmiljöer, vilket minskar risken för att utvecklings- och testarbete stör produktionen.

Sammankoppling av nätverk får endast ske efter att säkerhetsaspekterna analyserats och nödvändiga skyddsåtgärder vidtagits av respektive nätverks systemägare.

I samband med att information överförs genom data- och telekommunikation, uppkommer risker för avlyssning och förändring av den överförda informationen. Det ankommer på respektive IT-systems systemägare att analysera behov av, införa och dokumentera nödvändiga skyddsåtgärder för att hantera dessa risker.

Respektive systemägare, som nyttjar nätverken, definierar kraven på tillgänglighet, vilka ska ligga till grund för val av nätverksinfrastruktur.

Kablage, aktiva nätverkskomponenter och kommunikationsprotokoll ska väljas med utgångspunkt från verksamhetens krav på informationssäkerhet.

Datakommunikationen ska begränsas till vad som krävs för informationsutbytet.

6.3 Trådlösa nätverk

I samband med att information överförs med hjälp av trådlösa nätverk, uppkommer risker som kräver ytterligare skyddsåtgärder. Den påtagliga risken för avlyssning kräver att denna kommunikation krypteras.

Föreskrifter och instruktioner ska fastställas för design, konfiguration och användning av trådlösa nätverk.

Vid användning av trådlösa nätverk ska risken för störningar mot annan utrustning, som medicinteknisk utrustning, beaktas.

6.4 Landstingsgemensamma nätverk

Det ska fastsällas föreskrifter och instruktioner för anslutning till det landstingsgemensamma nätverket, SLLnet. Dessa ska gälla för alla organisationer som vill nyttja SLLnet, såväl landstingsinterna som externa, som för alla förekommande anslutningsformer.

Fjärranslutningar till IT-system för t.ex. fjärrdiagnostik eller -övervakning ska ske under kontrollerade former, fastställda av respektive systemägare. Anslutning, som inte sker via SLLnet, ska normalt vara nedkopplad och endast kopplas upp efter överenskommelse vid varje tillfälle.

6.5 Externa nätverk

Föreskrifter och instruktioner ska fastställas, som reglerar hur anslutning till externa nätverk och Internet ska ske och hur tillhandahållna tjänster får användas. För alla förvaltningar och bolag som nyttjar SLLnet, ska anslutningar till externa nätverk och Internet ske via SLLnet.

7 Systemutveckling och -anskaffning

7.1 Allmänt

Detta kapitel beskriver riktlinjer för informationssäkerhet i samband med utveckling och anskaffning av informationssystem, med syfte att säkerställa att kraven på informationssäkerhet beaktas.

Inga system får anskaffas eller utvecklas utan att det har gjorts en analys av hur systemet förhåller sig till bestämmelserna i Tryckfrihetsförordningen, Sekretesslagen, Arkivlagen, Personuppgiftslagen och andra lagar och regler som styr verksamheten.

7.2 Definition av säkerhetskrav

Vid upphandling av informationssystem, ny- och vidareutveckling av system i egen regi eller i samverkan med samarbetspartner, ska informationssäkerhetskraven definieras utifrån en riskanalys. Kraven på systemet ska tydligt framgå i kravspecifikationen.

7.3 Säkerhet i systemutvecklingsprojekt

I systemutvecklingsprojekt ska system och programvara skyddas på motsvarande sätt som de färdiga produkterna. Lämpliga skyddsåtgärder ska vidtas för att skydda källkoden och dokumentationen. Utvecklings- och testmiljöer ska vara separerade från produktionsmiljön.

7.3.1 Systemutvecklingsmodeller

Dokumenterade modeller för systemutveckling och projektstyrning ska finnas och tillämpas.

7.3.2 Ändrings- och versionshantering

För att säkerställa god spårbarhet, ska rutiner för ändrings- och versionshantering vara fastställda och användas inom projekten. Alla ändringar ska godkännas innan de genomförs.

7.3.3 Riktlinjer för test och kvalitetssäkring

Utdatas riktighet ska utvärderas under testfasen med hjälp av rimlighetskontroller. Test med produktionsdata ska undvikas. Användning av persondata, som kan härledas till identifierbara personer, får inte förekomma.

7.3.4 Riktlinjer för produktionssättning

Instruktioner för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas. System ska genomgå acceptanstest före godkännande av beställare. Det färdigtestade systemet ska därefter överlämnas för produktionssättning.

7.3.5 Utveckling av inbyggda kontroller

För att minska risken för fel i informationen, bör in- och utdata till system samt intern bearbetning kontrolleras med hjälp av automatiska valideringskontroller. Valideringskontrollerna ska utformas med hänsyn till de risker som identifierats i riskanalysen.

Automatiska kontroller kan även kompletteras eller ersättas med manuella avstämningskontroller efter behov.

7.4 Säkerhet vid upphandling av systemutveckling och system

I kravspecifikationen ska alltid ingå de i riskanalysen fastlagda informationssäkerhetskraven, en specifikation av i vilka tekniska miljöer och på vilka plattformar systemet ska fungera och krav på att systemets trafikkaraktäristik redovisas i anbudet.

7.4.1 Upphandling

Vid utläggning av systemutvecklig och anskaffning av standardsystem, ska ett formellt upphandlingsförfarande, enligt lagen om offentlig upphandling (LOU), genomföras. Landstingets upphandlingspolicy ska följas och avrop mot befintliga ramavtal i första hand göras.

Vid systemutveckling ska leverantören överlämna all information och programvara, som källkod, system- och driftdokumentation, samt dokumentation över krav på utvecklingsmiljö, till landstinget när uppdraget är avslutat, om inte annat är avtalat.

Avtal ska utformas så att beställaren erhåller fullständigt ägande, förfogande och upphovsrätt, samt övriga immateriella rättigheter samt till allt arbete och material som upp- eller tillkommit i samband med uppdraget. Om detta inte är möjligt bör avtal om deponering av källkod träffas.

Fysiskt överlämnande till beställaren s.k. tradition, måste ske för att besittningsövergång ska anses ha skett, vilket är nödvändigt för att skydda beställaren mot leverantörens borgenärer, i händelse av konkurs eller obestånd.

Landstinget ska därför sträva efter att få till stånd tradition av lös egendom, upphovsrätt till dataprogram och annat av immateriell rätt skyddat intellektuellt arbete, vilket tagits fram inom ramen för uppdraget.

7.4.2 Krav på leverantör

I förfrågningsunderlaget ska de krav som ställs på leverantören anges. Det gäller såväl krav på leverantörens ekonomiska och finansiella förmåga som krav på leverantörens tekniska förmåga och kapacitet. Reglerna i LOU kap.1 17 § ska följas. Förordning (1998:1364) om bevis vid offentlig upphandling, reglerar vilka krav som kan ställas på presumtiva anbudsgivare.

7.4.3 Anpassning av system

System bör så långt det är möjligt, användas utan modifiering eller anpassning. Eventuella anpassningar ska föregås av en analys av hur dessa kan komma att påverka informationssäkerheten. Analysen ska även inbegripa hur ändringarna påverkar avtalet med leverantören, med avseende på t.ex. ansvaret för icke förutsebara fel, som orsakas av ändringarna.

7.4.4 Leveransgodkännande

Instruktioner för acceptanstest, driftgodkännande och produktionssättning ska finnas och användas. Systemet ska genomgå acceptanstest före godkännande av beställare. Det färdigtestade systemet ska därefter överlämnas för produktionssättning.

7.5 Dokumentation

Utförlig system-, användar- och driftdokumentation ska framställas i utvecklingsprojektet. Vid systemanskaffning ska denna dokumentation tillhandahållas av leverantören. Fastställda rutiner ska finnas som säkerställer att dokumentationen uppdateras vid förändringar av systemet.

8 Fysisk säkerhet

8.1 Allmänt

Detta kapitel beskriver riktlinjer avseende den fysiska säkerheten för IT-system och informationstillgångar i landstingets egna lokaler såväl som i förhyrda. Den fysiska säkerheten syftar till att skydda mot obehörigt tillträde och åtkomst, skador och störningar.

8.2 Riktlinjer för skydd av utrustning och information

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

För verksamheten kritiska IT-system och informationstillgångar ska inrymmas i säkra utrymmen, omgärdade av skalskydd, med lämpliga tillträdesspärrar och -kontroller.

8.3 Tillträdeskontroll till byggnader och lokaler

Vid behov ska tillträdeskontroll till viktiga byggnader och lokaler finnas, för att säkerställa att endast behörig personal ges tillträde.

8.4 Skydd i säkra utrymmen

Med säkra utrymmen avses utrymmen som är speciellt uppbyggda för att uppfylla högre krav på skal- och brandskydd samt säker tillgång till el och kyla.

För att säkerställa att endast behörig personal ges tillträde till säkrade utrymmen, ska dessa skyddas med hjälp av lämpliga tillträdeskontroller.

8.4.1 Skalskydd

Skalskyddet ska omfatta väggar, dörrar, fönster, tak och golv. Skalskyddet bör byggas upp i flera nivåer.

8.4.2 Tillträdesskydd

Entréer ska skyddas med bemannade receptioner eller datoriserade passagekontrollsystem, med möjlighet att använda individuella passagekort och till dessa kopplade koder, vilket ger möjlighet att logga in- och utpasserande.

Om det i övrigt har installerats passagekontrollsystem, bör ur kostnads- och effektivitetssynpunkt också de säkra utrymmena anslutas till samma system. De speciella krav på begränsning av tillträdet som kan finnas, per individ, tid på dygnet etc., måste dock kunna tillgodoses. Fastställda rutiner för uppföljning av loggar ska finnas och tillämpas.

För att uppnå full effekt av tillträdesskyddet, bör det integreras med inbrottslarm.

8.4.3 Brandskydd

Datorer och annan elektronisk utrustning, som lagringsmedia, är känsliga för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns.

8.4.4 Vattenskydd

Rör, där vatten står under tryck, bör inte finnas i säkra utrymmen. Vätskelarm ska finnas, om det i utrymmet finns rördragningar innehållande vatten, eller om det av andra orsaker finns risk för vattenskada.

8.4.5 Klimatanläggning

Verksamhetskyla ska finnas som motsvarar den överskottsvärme som alstras av utrustningen.

8.5 Kraftförsörjning och el-miljö

Elektronisk utrustning bör skyddas mot elavbrott och andra störningar i elförsörjningen. Strömförsörjning av verksamhetskritiska system och utrustningar, bör ske via avbrottsfri kraftmatning (UPS), som i sin tur bör anslutas till reservkraft.

Risker rörande den elektromagnetiska miljön bör beaktas.

8.6 Underhåll av utrustning

Leverantörens rekommenderade underhållsplan för utrustningen ska i första hand följas.

8.7 Säkerhet för utrustning utanför egna lokaler

Risker i samband med hantering av utrustning utanför de egna lokalerna ska beaktas. Detta gäller för informationsbärare i vid mening och omfattar bland annat persondatorer, handdatorer, mobiltelefoner och pappersdokument. Instruktioner ska fastställas för hur sådan utrustning ska hanteras.

Vid utformning av skyddsåtgärder måste det beaktas att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter. Viktigt är att även beakta riskerna då utrustning lämnas ut för extern service.

Utförsel av utrustning, som innehåller känslig information, ska godkännas av informationsägaren och registreras.

8.8 Avveckling av utrustning

Lagringsmedia, som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning.

9 Personal och informationssäkerhet

9.1 Allmänt

Detta kapitel beskriver riktlinjer för informationssäkerhet som ska tillämpas inom personalprocessen dvs. i samband med rekrytering, anställning och avslutande av anställning.

9.2 Arbetsbeskrivning och anställningsvillkor

Av anställningsvillkoren ska framgå den anställdes skyldighet att uppfylla de krav som ställs i landstingets informationssäkerhetspolicy, dessa riktlinjer och, med stöd av riktlinjerna, fastställda föreskrifter och instruktioner.

Samtliga anställda ska göras medvetna om sina skyldigheter enligt anställningsavtalet samt informeras om gällande regler för informationssäkerhet och sekretess.

I anställningsvillkoren ska det också anges att bristande efterlevnad av informationssäkerhets-policy, riktlinjer, föreskrifter och instruktioner kan vara misskötsel, vilket är ett brott mot anställningsavtalet.

Motsvarande ska i förekommande fall regleras i avtal med uppdragstagare, som inte är anställda.

9.3 Rekrytering

Vid rekrytering ska kontroll och uppföljning av den arbetssökandes referenser och formella meriter, som CV, meritförteckning och yrkeslegitimationsinnehav, göras. En kontroll av den sökandes identitet ska också genomföras, för att klargöra att personen verkligen är den som den utger sig för att vara. Vid behov, och efter den arbetssökandes samtycke, ska drogtest genomföras och kreditupplysning inhämtas. Detsamma ska gälla vid anlitande av tillfällig personal för känsliga befattningar.

Särskild säkerhetsprövning ska ske innan en person, genom anställning eller på annat sätt, deltar i verksamhet som har betydelse för rikets säkerhet eller skyddet mot terrorism. Den som säkerhetsprövningen gäller ska ha gett sitt samtycke innan registerkontroll och särskild personutredning får göras. Ett samtycke ska anses gälla också förnyade kontroller och utredningar så länge som den kontrollerade innehar samma anställning.

Vid rekrytering registreras ofta personuppgifter i informationssystem. Endast sådana uppgifter som är nödvändiga för registrets ändamål får behandlas. Om det i lag eller annan författning finns särskilda kompetenskrav för en viss anställning kan det vara nödvändigt att behandla sådana uppgifter. I samband med att rekryteringen avslutas ska uppgifterna i registret tas bort.

Närmare anvisningar finns att hämta i Datainspektionens skrift Personuppgifter i arbetslivet.

9.4 Bisysslor

Lagen om offentlig anställning innehåller bestämmelser om skyldighet för offentliga arbetsgivare att informera anställda om vilka slags förhållanden som kan göra en bisyssla otillåten, enligt bestämmelsen om förbud mot förtroendeskadliga bisysslor.

Denna vägledning kan finnas på papper eller vara tillgänglig för arbetstagarna i elektronisk form t.ex. via ett s.k. intranät. Frågan om bisysslor bör också beröras muntligt vid anställning och vid personalinformation.

Den anställde är skyldig att på arbetsgivarens begäran lämna de uppgifter som behövs för att arbetsgivaren ska kunna bedöma den anställdes bisysslor. Uppgiftsskyldigheten omfattar alla slags bisysslor.

I kollektivavtalet, Allmänna bestämmelser, finns ytterligare regler om bisysslor.

9.5 Sekretess

Inom den offentliga sektorn är sekretess för de anställda reglerat i lag. En sekretessförbindelse är därför inte möjlig att använda, utan ersätts av sekretesserinran. Denna skrivs inte under utan, som namnet säger, erinrar om gällande lagstiftning.

Man behöver inte vara anställd av landstinget eller dess företag för att omfattas av sekretessen. Vid anlitande av konsult eller annan extern uppdragstagare måste emellertid klargöras om han eller hon deltar i verksamheten på samma sätt som en anställd.

Deltar personen inte i verksamheten på sådant sätt att sekretesslagen blir tillämplig, ska tystnadsplikten regleras civilrättsligt, dvs. i avtal.

9.6 Avslutande av anställning

Det ska finnas fastställd rutin för hantering av personal som avslutar sin anställning inom landstinget. Rutinen ska säkerställa att åtkomsträttigheter upphör vid anställningens slut. Den ska även säkerställa att nycklar, passerkort och övrig utrustning återlämnas.

9.7 Utbildning och fortbildning i informationssäkerhet

Landstingets målsättning är att ge samtliga anställda den utbildning i informationssäkerhet som krävs, för att dessa ska kunna utföra sina arbetsuppgifter och för att säkerställa informations-säkerhetsmålet.

En anställd kan oavsiktligt åsamka organisationen stor skada på grund av bristande kunskap. Det är därför viktigt att introduktion och utbildning om gällande regler för informationssäkerhet genomförs för nya anställda.

Detsamma gäller även vid omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen.

Utbildningen bör följas upp årligen. I samband med uppföljningen bör en omvärldsanalys eller annan aktuell information inom området presenteras. Rapporterade incidenter och resultatet från genomförda riskanalyser bör också presenteras.

10 Kontinuitetsplanering

10.1 Allmänt

Detta kapitel beskriver riktlinjer för kontinuitetsplanering, dvs. den planeringsprocess som syftar till att säkerställa verksamhetens kontinuitet.

10.2 Kontinuitetsplaneringens mål

Målet med kontinuitetsplaneringen är att kritiska verksamhetsprocesser ska kunna upprätthållas, på rimlig nivå, vid olika typer av oförutsedda störningar och avbrott.

10.3 Kontinuitetsplaneringens omfattning

Kontinuitetsplaner ska utformas för verksamhetens kritiska processer. För att uppnå en god kontinuitet, krävs en kombination av förebyggande och återställande skydd.

Planerna ska innefatta samtliga de åtgärder som i förväg kan vidtas, för att säkerställa verksamhetens kontinuitet.

I kontinuitetsplaneringen ska ingå att identifiera risker, begränsa konsekvenser av händelser och säkerställa återgång till normal drift för viktiga verksamheter inom rimlig tid. Följderna av eventuella incidenter, katastrofer och förlust av verksamhetsstöd ska analyseras.

Baserat på verksamhetens krav på tillgång till information och genomförda riskanalyser, ska planer för att hantera avbrott i de IT-system som stödjer verksamhetens kritiska processer utformas. När avbrott, planerade och oplanerade, inträffar, ska det finnas fastställda reservrutiner som hanterar detta. Dessa rutiner kan vara såväl manuella som IT-baserade.

De delar av kontinuitetsplaneringen som berör katastrof- och beredskapssituationer ska ingå i verksamhetens övriga katastrofplanering.

Beredskapsförordningen ställer särskilda krav på verksamheten vid beredskapsmyndigheter.

10.4 Test och underhåll

Kontinuitetsplanerna ska testas regelbundet, minst årligen, enligt fastställd plan. Planerna ska underhållas genom regelbundna granskningar och övningar, för att säkerställa att de är aktuella och ändamålsenliga.

11 Uppföljning och efterlevnad

11.1 Allmänt

Detta kapitel beskriver lagar och andra författningar som påverkar landstingets verksamheter med avseende på informationssäkerheten. Dessutom anges riktlinjer för granskning av efterlevnad av informationssäkerhetspolicy, riktlinjer, föreskrifter och instruktioner liksom utvärdering och uppdatering av dessa, i syfte att säkerställa att de är aktuella och tillräckliga.

11.2 Legala och externa krav

Landstingets verksamhet är av skiftande karaktär och bedrivs i olika organisationsformer. Minimikraven på informationssäkerheten ställs genom författningar i form av lagar, förordningar och myndighetsföreskrifter. Varje förvaltning och bolag ansvarar för att uppfylla de författningar som respektive verksamhet styrs och påverkas av.

I de föreskrifter, som enligt dessa riktlinjer ska utformas inom respektive förvaltning och bolag, ska de författningar identifieras, som påverkar informationssäkerheten.

Nedan beskrivs, utan anspråk på fullständighet, författningar som kan ha påverkan på informationssäkerheten inom landstinget.

11.2.1 Insynslagstiftningen

Med insynslagstiftningen avses primärt reglerna i 2 kapitlet tryckfrihetsförordningen, om allmänna handlingars offentlighet, och 15 kapitlet sekretesslagen, om registrering och utlämnande av allmänna handlingar.

Allmänhetens rätt att ta del av allmänna handlingar enligt tryckfrihetsförordningen, den s.k. offentlighetsprincipen, gäller för alla inkomna och upprättade handlingar. Även arkivlag-stiftningen innehåller bestämmelser som syftar till att uppfylla offentlighetsprincipen.

Offentlighetsprincipen, liksom sekretesslagen och arkivlagen, gäller också bolag, föreningar och stiftelser där landstinget har ett avgörande inflytande.

Instrumenten för allmänhetens insyn är registreringen av handlingar och beskrivning av ADB-register, liksom arkivbeskrivning och arkivförteckning.

Lagen om överlämnande av allmänna handlingar för förvaring till andra organ än myndigheter, förvaringslagen, kan i vissa fall tillämpas om myndigheten ska läggas ned, upphöra med viss verksamhet eller verksamheten ska övergå i annan driftform, t.ex. i samband med bolagisering. Då allmänna handlingar ska förvaras hos tredje part, ska landstingsarkivet kontaktas.

11.2.2 Integritetsskyddslagstiftningen

I första hand avses reglerna om tystnadsplikt i sekretesslagen och -förordningen, samt bestämmelserna i personuppgiftslagen med anknytande registerförfattningar, som vårdregisterlagen. De senare tar främst sikte på automatiserad behandling av personuppgifter, dvs. uppgifter som kan härledas till levande person, och är straff- och skadeståndssanktionerade.

Datainspektionen har utfärdat allmänna råd om bl.a. säkerhet för personuppgifter och information till registrerade enligt personuppgiftslagen. I inspektionens skrift, Information om vårdregisterlagen, berörs vissa informationssäkerhetsfrågor gällande vårdregister.

Hanteringen av uppgifter, som rör dem som inom folkbokföringen fått skyddade personuppgifter, nödvändiggör särskilda rutiner. Uppgifterna får bara hanteras i sådan verksamhet där sekretess råder. För att garantera att de individer som fått skyddade personuppgifter inte exponeras, ska rutinerna fastställas i föreskrifter eller instruktioner. Dessa ska vara utformade så att kretsen av personer som har behörighet att ta del av uppgifterna begränsas så mycket som möjligt, och ska på ett heltäckande sätt ange förutsättningarna för hanteringen av uppgifterna.

Även annan lagstiftning kan sägas ha integritetsskyddande syfte, som t.ex. brottsbalkens straffbestämmelser, lag om elektroniska anslagstavlor, lag om kvalificerade elektroniska signaturer, säkerhetsskyddslagen och lag om företagshemligheter.

Även reglerna om meddelarfrihet, som genom sekretesslagen är kraftigt inskränkt på hälso- och sjukvårdens område, och om ansvarig utgivare i tryckfrihetsförordningen och yttrandefrihetsgrundlagen, rymmer integritetsskyddsaspekter.

Rättegångsbalkens regler om begränsad möjlighet för vissa yrkesgrupper, som hälso- och sjukvårdspersonal, att som vittne uttala sig om vad de anförtrotts eller erfarit i samband med yrkesutövning, kan också sägas ha integritetsskyddande syfte.

11.2.3 Annan överordnad lagstiftning

Bland övriga författningar som styr landstingets verksamhet och som har påverkan på informationssäkerheten, kan särskilt framhållas kommunallagen, förvaltningslagen, aktiebolagslagen, lag om offentlig upphandling (LOU), bokföringslagen och -förordningen respektive lag om kommunal redovisning.

Jävsregler för tjänstemän och ledamöter inom det kommunala området finns i kommunallagen. Vissa särregler finns för bolag i vilka landstinget äger minst hälften av aktierna och stiftelser där landstinget utser minst hälften av styrelseledamöterna.

Upphovsrättslagen, patentlagen, lag om rätten till arbetstagares uppfinningar, liksom andra lagar på det immaterialrättsliga området, berör också informationssäkerheten.

11.3 Verksamhetsspecifik lagstiftning

11.3.1 Hälso- och sjukvård

Av de författningar som påverkar hälso- och sjukvården, och som berör informationssäkerheten, bör, förutom de överordnade reglerna i sekretesslagen och personuppgiftslagen, särskilt nämnas patientjournallagen, vårdregisterlagen, lag om hälsodataregister och biobankslagen.

Till ovan nämnda författningar kommer bl.a. de mera allmänna bestämmelserna i hälso- och sjukvårdslagen, tandvårdslagen och -förordningen, liksom lag och förordning om yrkesverksamhet på hälso- och sjukvårdens område. Bestämmelser om tvång i vården förkommer i lagstiftningen om psykiatrisk tvångsvård och rättspsykiatrisk vård liksom i smittskyddslagen.

Patientskadelagen, lagen om kommunalt betalningsansvar för medicinskt färdigbehandlade och förordning om verksamhetschef inom hälso- och sjukvården är också relevanta.

Flera av de nämnda författningarna kompletteras av föreskrifter och allmänna råd från Socialstyrelsen, som har bärighet på informationssäkerhet. Detta gäller t.ex. föreskrifter och allmänna råd om samordnad vårdplanering på äldrevårdens område, kvalitetssystem, läkemedelshantering, journalföring, rättsintyg vid utredning av vålds- och sexualbrott, verksamhetschef, biobanker, tvångsvård, smittskydd, lokal avvikelsehantering, ”Lex Maria”, identitetskontroll och åtgärder för att förhindra förväxling.

Regler finns också om anmälnings- och uppgiftsskyldigheter som kan bryta annars gällande sekretess. Detta gäller i vissa särskilt författningsreglerade fall gentemot bl.a. socialtjänsten, polis- och åklagarmyndighet, Migrationsverket, Överförmyndaren och Socialstyrelsen. I förordningen om verksamhetschef regleras dennes ansvar bl.a. om person som lämnar eller avser att lämna sjukvårdsinrättning är farlig för sin egen eller annans personliga säkerhet.

11.3.2 Trafik

Landstinget är trafikhuvudman i länet både för den allmänna kollektivtrafiken och för den särskilda kollektivtrafiken, färdtjänsten. Tunnelbane-, spårvägs- och järnvägstrafik regleras av ett antal bestämmelser. Järnvägssäkerhetslagen, med tillhörande föreskrifter från järnvägs-inspektionen, ställer bl.a. krav på fastställda rutiner för säkerhetsstyrning, spårbarhet avseende information och informationssystem som hanterar hälso-, kompetens- och fortbildningsstatus hos egen personal och anlitade entreprenörer.

I färdtjänstlagen finns regler om särskilt anordnade transporter för personer med funktionshinder som bl.a. berör möjligheten att lämna ut uppgifter om enskildas personliga förhållanden till en beställningscentral för transporter eller en trafikutövare och tystnadsplikt för enskilda yrkesutövare.

Genom Waxholms Ångfartygs AB har landstinget ansvar för beställning av den kollektiva sjötrafiken i skärgården och i Stockholms hamn. Även denna verksamhet regleras genom säkerhetsrelaterad lagstiftning.

11.3.3 Säkerhetsskydd

Säkerhetsskyddslagen och -förordningen liksom Rikspolisstyrelsens föreskrifter om säkerhetsskydd (FAP 244-1), reglerar myndigheters åtgärder för att förebygga spionerі, sabotage, terrorism och andra brott som kan hota rikets säkerhet, liksom för att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet.

11.3.4 Kris och krig

Lagen om extraordinära händelser i fredstid hos kommuner och landsting innebär bl.a. att en krisledningsnämnd får fatta beslut om att överta hela eller delar av verksamhetsområden från övriga nämnder i landstinget, i den utsträckning som är nödvändig, med hänsyn till den extraordinära händelsens art och omfattning.

Krigsutskottet är landstingsstyrelsens krigsorganisation och övertar vid högsta beredskap, enligt lag om höjd beredskap, landstingsstyrelsens uppgifter. Föreskrifter om den kommunala organisationen under krig eller krigsfara finns i lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara.

Krisberedskapsmyndigheten har det sammanhållande myndighetsansvaret för samhällets informationssäkerhet. När en kris inträffar hamnar ofta informationsfrågorna i fokus. Krisberedskapsmyndigheten arbetar för att den drabbade kommunen eller myndigheten ska ha en god beredskap och förmåga att kommunicera med medborgare, medier och andra kommuner och myndigheter när en kris inträffar. Eftersom Krisberedskapsmyndigheten har tagit över viss verksamhet från Överstyrelsen för civil beredskap (ÖCB) och Styrelsen för psykologiskt försvar (SPF) bör även material från dessa myndigheter beaktas.

11.4 Uppföljning av informationssäkerheten

11.4.1 Uppföljning av regelverket

För att säkerställa att de säkerhetskrav och skyddsåtgärder som beskrivs i policy, dessa riktlinjer, föreskrifter och instruktioner, är aktuella och tillräckliga med hänsyn till förändringar i verksamhet och omvärld, ska befintliga såväl som nya risker kartläggas med hjälp av riskanalyser och skyddsåtgärdernas verkan löpande utvärderas genom t.ex. sårbarhetsanalyser.

Omvärldsanalysen ska innefatta IT-utvecklingen, ny eller förändrad lagstiftning, standarder, marknadskrav, annan teknikutveckling etc.

Baserat på resultatet från dessa analyser ska anpassningar av regelverket göras.

Landstingsdirektören ska, på informationssäkerhetschefens initiativ, anhängiggöra ärende om ändring av informationssäkerhetspolicyn eller av dessa riktlinjer.

11.4.2 Uppföljning av efterlevnad

Informationssäkerheten ska regelbundet följas upp, såväl på central nivå som inom respektive förvaltning och bolag.

För att säkerställa att regelverket efterlevs, ska det årligen, och så snart händelser som påverkar informationssäkerheten inträffat, genomföras oberoende granskning. Denna kan initieras av landstingets informationssäkerhetsorganisation eller av landstingets revisorer; på eget initiativ eller inom ramen för planerad revision.

Varje förvaltning och bolag ska dessutom regelbundet granska sin informationssäkerhet och därvid inventera installerade system samt göra en analys av hur systemen förhåller sig till författningar och andra regler som styr verksamheten.

Baserat på genomförda granskningar och identifierade avvikelser, ska skyddsåtgärder anpassas och kompletteras.