Universitetsledningens kansli 2020-04-01

Samordnare informationssäkerhet

# Ledningssystemet för informationssäkerhet vid Umeå universitet

## 1. Inledning

Information är en av universitetets viktigaste tillgångar och en förutsättning för att verksamheten ska fungera. Informationen måste därför göras tillgänglig och skyddas från att till exempel läcka ut, förvanskas eller förstöras. Universitetets informationstillgångar måste därför skyddas så att:

- Informationen alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av informationen (konfidentialitet) och
- att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet)

En säker informationshantering utgör en förutsättning för att Umeå universitet skall kunna fullgöra uppdraget med att tillhandahålla utbildning, bedriva forskning samt att samverka med det omgivande samhället. Grunden till säker informationshantering utgörs av ledningssystem som hjälper ledningen att styra informationssäkerhetsarbetet, hjälper säkerhetsfunktionen vid universitetet att utforma säkerhetsåtgärder och utbilda universitetets anställda, samt möjliggör ständiga förbättringar i området.

## 2. Ledningssystemets övergripande syfte, struktur och innehåll

Strukturen på ledningssystemet består av fyra (4) områden som tillsammans ska ses som en kontinuerlig process med sina specifika övergripande syften (fig. 1) och rollbeskrivningar.

**Ledning och styrning:**

*Förståelse för universitetets behov och nödvändigheten att styra informationssäkerhetsarbetet mot uppsatta informationssäkerhetsmål.*

**Verksamhetsanalys:**

*Tillämpning och hantering av processer för informationssäkerhet, säkerhetsåtgärder och andra mått för att säkerställa en för universitetet lämplig säkerhetsnivå i it-resurser.*

**Utbildning och övning:**

*Vidta åtgärder för att ge anställda möjlighet att få utbildning i informationssäkerhet*

**Utvärdering och förbättring:**
*Ständiga förbättringar genom uppföljning av genomförda aktiviteter.*

Innehållet i ledningssystemet har sin grund i ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna ISO/IEC 27001/2 och myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters arbete med informationssäkerhet. Universitetets ledningssystem omfattar 16 aktiviteter fördelade på 4 fokusområden enligt fig 1.

| Ledning och styrning | Verksamhetsanalys | Utbildning & övning | Utvärdering & förbättring |
|---|---|---|---|
| Genom ledningssystemet tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete | Klassificera information med utgångspunkt i krav på konfidentialitet, tillförlitlighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd | Informera medarbetare om krav på säker informationshantering och relevanta regler inom området | Fortlöpande dokumentera vidtagna åtgärder |
| Genom ledningssystemet tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver | Identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster | Regelbundet, och enligt en beslutad utbildningsplan, genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas arbetsuppgifter | Följa upp och utvärdera vidtagna åtgärder och gjorda bedömningar av hot och risker |
| Genom ledningssystemet säkerställa att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas | Utifrån informationsklassningens resultat och genomförd riskanalys identifiera och vidta de åtgärder som krävs för att uppfylla skyddsbehovet | Regelbundet, och enligt en beslutad övningsplan, genomföra övningar för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet | Kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet |
| Upprätta en informationssäkerhetspolicy och andra styrande dokument | Tillse att det finns rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för | | |
| Årlig handlingsplan | Tillse att det finns rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott | | |

*Figur 1. Ledningssystemets omfattning och innehåll*

## Roller

**Rektor** utser ansvarig för samordningen av informationssäkerheten. I enlighet med rektors delegationsordning är det universitetsdirektören som har till uppgift att leda och samordna arbetet med universitets informationssäkerhet och är därmed informationssäkerhetsansvarig. Universitetsdirektören eller den eller de som denna delegerar till, har som informationssäkerhetsansvarig ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerhetsarbetet

**Informationssäkerhetsansvarig** har ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av universitets arbete med informationssäkerhet. Informationssäkerhetsansvarig är universitetsdirektören eller den eller de som denne delegerar till.

**Informationssäkerhetsgruppen** är ett stöd till den informationssäkerhetsansvariga. Gruppen är ett rådgivande beredande organ inom informationssäkerhetsarbetet, och har bland annat ansvar för att se till att ledningssystemet för informationssäkerhet vid Umeå universitet fungerar och efterlevs i alla delar.

**Dekan, prefekt eller enhetschef** har ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerheten vid sin fakultet, institution, centrum eller enhet. Prefekt och enhetschef har ansvar för att informationstillgångens konfidentialitet, tillgänglighet och riktighet upprätthålls genom att tillse att informationsklassningar och risk & sårbarhetsanalyser genomförs.

För att ledningssystemet för informationssäkerhet ska vara verkningsfullt i arbetet med ständiga förbättringar inom informationssäkerhet ska informationsägaren arbeta med följande checklista för årlig nulägesbedömning:

- Risk och sårbarhetsanalyser – vad har hänt med eventuella åtgärder? Är arbete med åtgärder inplanerade?
- Har det genomförts större förändringar i system/driftmiljöer som kan ha påverkan på säkerheten?
- Har det förekommit några incidenter som bör leda till reviderade bedömningar av säkerhetsläget?
- Har institutionen utökats med nya it-system/it-tjänster/lagringslösningar? Har det i så fall gjorts informationsklassning och risk och sårbarhetsanalys?
- Genomförs det kontinuerliga åtkomst och behörighetskontroll till it-system
- Rapportering till samordnare informationssäkerhet enligt anvisning

**Samordnare informationssäkerhet** ansvarar för den operativa driften och samordningen av ledningssystemet och dess aktiviteter.

**IT-säkerhetsansvarig** ansvarar för IT-säkerhet i infrastruktur, serversystem och klientdatorer.

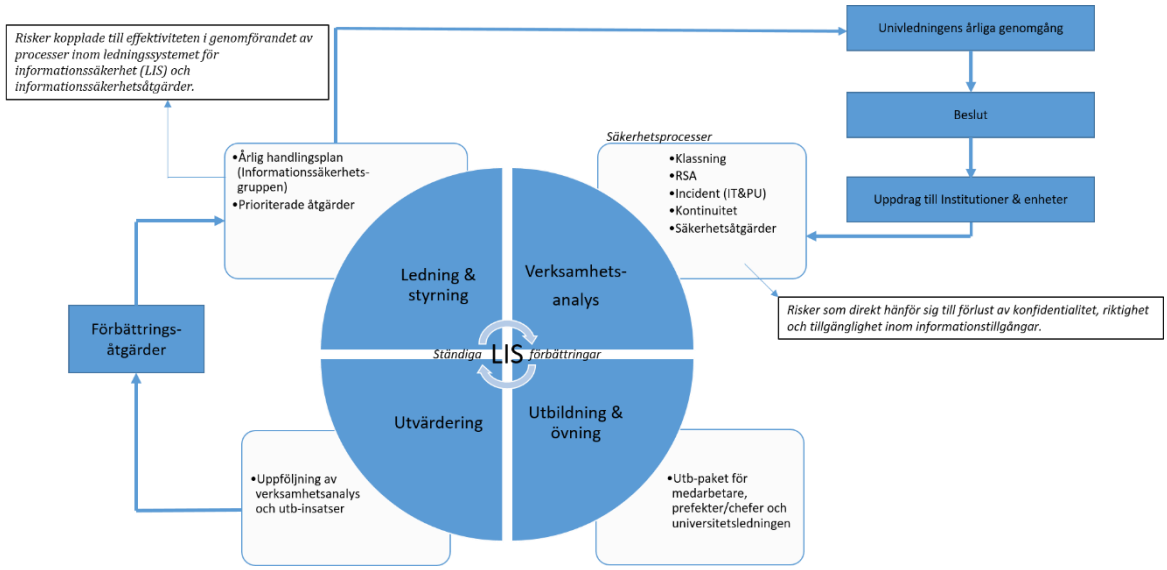
**Incident response team IRT inom ITS** ansvarar för förebygga, upptäcka och utreda IT-säkerhetsincidenter på Umeå universitet.

**Säkerhetschef och samordnare LOK** ansvarar för den fysiska säkerheten vid universitetet och är behjälplig med anvisningar och riktlinjer samt utbildningsinsatser vid institutioners arbete med riskanalyser, åtgärdsplaner och genomförande.

# 3. LIS som kontinuerlig process

Ledning och styrning av informationssäkerhet ska ligga i linje med universitetets sätt att i övrigt leda och styra verksamheten. Konkret handlar det om att samordna aktiviteter, metoder och rutiner för att tillförsäkra att system och information omfattas av säkerhetsaspekterna konfidentialitet, tillgänglighet samt riktighet.

*Ledning och styrning* (fig.2) omfattar bl. a. att årligen analysera gällande lagstiftning och gällande föreskrifter samt planera nästkommande års prioriterade arbete med informationssäkerhet. Här ingår prioritering av identifierade förbättringsåtgärder samt beredning av den årliga genomgången med universitetsledningen. Arbetet sker på en universitetsövergripande nivå med stöd av en arbetsgrupp (universitetets informationssäkerhetsgrupp) bestående av representanter för universitetsförvaltning och övrig verksamhet under ledning av informationssäkerhetsansvarig eller den till vilken denna delegerar uppgiften. Ledning och styrning sker på två nivåer. 1.) Universitetet identifierar risker och åtgärder som dokumenteras i årlig handlingsplan för informationssäkerhet, och 2.) en operationaliserad handlingsplan som explicit fokuserar på ledningssystemets kontinuerliga aktiviteter i delarna verksamhetsanalys och utbildning.




*Figur 2. Ledningssystemets övergripande struktur samt aktiviteter*

Efterföljande fas – *verksamhetsanalys* – innefattar aktiviteter för att genomdriva det faktiska informationssäkerhetsarbetet. Aktiviteterna är: informationsklassning och risk & sårbarhetsanalys som utifrån respektive resultat fastställer tekniska och organisatoriska säkerhetsåtgärder. Incidenthantering genomförs enligt fastställd process och omfattar IT-säkerhetsincidenter såväl som personuppgiftsincidenter samt kontinuitetshantering. Handläggningsordningar, processer och rutiner finns för arbete i denna fas. Detta inkluderar även säkerhet i personuppgiftsbehandling.

*Utbildning och övning* - Anställda utbildas/informeras om informationssäkerhetsansvaret utifrån befattning och ansvar. Prefekter, enhetschef, föreståndare informeras om sitt informationssäkerhetsansvar åtminstone en gång per år i samband med prefekt-/chefsträffar. Systemadministratörer och IT-kontaktpersoner informeras om informationssäkerhetsfrågor åtminstone en gång per år i samband med respektive nätverksträffar. Övriga anställda informeras via Aurora. Webbaserad utbildning finns också på aurora.

*Utvärdering* - En periodisk återkommande uppföljning av genomförda aktiviteter är viktig för att bevaka ledningssystemets tillämplighet, verkan och effekt vid Umeå universitet. Utvärdering syftar till att åstadkomma förbättringsåtgärder som behandlas i informationssäkerhetsgruppen där prioriteringar görs i den årliga handlingsplanen.

# 4. Riskbaserat ledningssystem

Risker kopplade till effektivitet i genomförande av processer i ledningssystemet ska identifieras varje år för att formulera åtgärder i universitetets årliga handlingsplan för informationssäkerhet. Enligt strukturen i ISO/IEC 27001 delas risker upp i två kategorier:

1. risker och möjligheter som är relevanta för avsedda resultat av ledningssystemet för informationssäkerhet i sin helhet,

2. informationssäkerhetsrisker som hänför sig till förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystemet för informationssäkerhet.

De risker som hör till den första kategorin är normalt risker som hänför sig till själva ledningssystemet för informationssäkerhet, tillämpbarheten av ledningssystemet för informationssäkerhet, högsta ledningens engagemang för informationssäkerhet, resurser för drift av ledningssystem för informationssäkerhet etc.

De möjligheter som faller inom denna kategori kan vara möjligheter relaterade till resultat för ledningssystem för informationssäkerhet, värdet för universitetet av ett ledningssystem för informationssäkerhet, effektiviteten i genomförandet av processer inom ledningssystemet för informationssäkerhet och informationssäkerhetsåtgärder etc.

Den andra kategorin består av alla risker som direkt hänför sig till förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystemet för informationssäkerhet. Det vill säga de risker som identifieras genom informationsklassning och risk- och sårbarhetsanalys i forskningsprojekt, vid upphandling och utveckling av it-system, behandling av personuppgifter etc.

# 5. ISO-standarder för ledningssystem för informationssäkerhet

Standarder kring informationssäkerhet har samlats i standardserien 27000 och fokus är det systematiska arbetet med informationssäkerhet.

Standarderna är strukturerade i tre nivåer: krav, riktlinjer och stöd. Dessa olika nivåer visar vad (krav) en organisation bör göra när det gäller informationssäkerhet samt hur (riktlinjer och stöd) man kan arbeta.

De grundläggande standarderna i 27000-serien är:

- SS ISO/IEC 27000 Översikt och terminologi beskriver de standarder som ingår i 27000-serien. Här finns också de termer som används i de övergripande standarderna på informationssäkerhetsområdet samlade.
- SS-EN ISO/IEC 27001:2017 Ledningssystem för informationssäkerhet – Krav är den standard som beskriver ledningssystemet och som man kan certifiera sig mot.
- SS-EN ISO/IEC 27002:2017 Ledningssystem för informationssäkerhet – Riktlinjer beskriver vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla. Kapitlen i 27002 har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet, organisation och efterlevnad.
- ISO/IEC 27003:2017 Information Technology – Security Techniques – Information Security Management Systems – Guidance ger vägledning i hur en organisation kan uppfylla kraven i 27001.

Tabellen nedan visar säkerhetsåtgärder som kravställs i ISO 27001, bil A. Kvalitetsarbetet som görs med hjälp ledningssystemet eftersträvar att implementera säkerhetsåtgärderna för att utveckla informationssäkerhetsarbetet på bredden inom verksamhetsskyddet.

| Säkerhetsåtgärder | Avsnitt ISO27001 |
|---|---|
| Regelverk för informationssäkerhet och rutin för granskning av regelverket | A5 |
| Universitetet har säkerhetsåtgärder på plats för användande av mobila enheter och distansarbete | A6 |
| Medarbetare har grundläggande kunskap om informationssäkerhet, t.ex via MSB:s film som ligger på Aurora, och har kännedom hur it- och personuppgiftsincidenter rapporteras | A7, A16 |
| Skyddsnivåer för universitetets information (verksamhetsdata, forskningsdata) bestäms med informationsklassning | A8 |
| Universitetet har rutiner för behörighetsstyrning | A9 |
| Universitetet har krypteringslösning för datalagring och dataöverföring | A10, A13 |
| Data och licenserade programvaror har avlägsnats eller säkert överskrivits för destruering av it-utrustning | A11 |
| Universitetet har: skydd mot skadlig kod, säkerhetskopiering, loggning av it-händelser | A12 |
| Universitetet har skydd av datornätverk och it-system som motsvarar skyddsnivåer för verksamhetens olika informationstyper | A13 (ref. A8) |
| Universitetet ställer informationssäkerhetskrav vid upphandling av it-system | A14 |
| Universitetet har skydd för alla informationstillgångar och it-resurser som externa aktörer har åtkomst till | A15 |
| Universitetet har kontinuitetshantering för styrning av informationssäkerhet vid kris- eller katastrofsituationer | A14 |

Genom att universitetet bedriver arbetet med informationssäkerhet enligt ISO-standarderna kan universitetet realisera följande nyttoaspekter:

**Efterlevnad**: Universitetet säkerställer att legala krav efterlevs och revisioner klaras bättre. Det kan gälla exempelvis skydd av personuppgifter i enlighet med dataskyddsförordningen och krav på internkontroll.

**Styrning**: Universitetsledningen får möjlighet att styra och följa upp informationssäkerheten så att man kan bevaka att skyddet är effektivt och ändamålsenligt.

**Kommunikation**: Universitetet ansluter sig till ett vedertaget sätt att arbeta med informationssäkerhet och anammar en gemensam terminologi. Därigenom blir det lättare, och ofta en förutsättning för, att kommunicera och samarbeta om gemensamma informationssäkerhetsfrågor med kollegor vid andra lärosäten och organisationer.

**Ekonomi**: Universitetet får en god informationssäkerhet som är anpassad efter verksamhetens förutsättningar och behov. Universitetet får en bra säkerhetsekonomi genom att säkerhetsincidenter kan undvikas via ett väl avpassat, ändamålsenligt och kostnadseffektivt skydd.

**Förtroende**: Genom säkerhet i informationshanteringen kan omvärldens förtroende för Umeå universitet bibehållas och öka.