Typ av dokument: Policy
Beslutad av: Rektor
DNR: FS.1.1.1-998-17
Giltighetstid: 2017-06-13 - tills vidare
Område: Organisation
Ansvarig enhet: Planeringsenheten

Informationssäkerhetspolicy för Umeå universitet

Inledning

Denna policy utgör grunden i universitetets ledningssystem för informationssäkerhet (LIS) och beskriver Umeå universitets ramverk för informationssäkerhet. Policyn ska utgöra ett stöd för verksamheten i det dagliga arbetet. Arbetet med informationssäkerhet utgår främst från lagar, förordningar, föreskrifter, universitetets egna krav samt avtal. Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) har använts som utgångspunkt för föreliggande policy. Enligt dessa föreskrifter ska myndigheten:

- Bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas.
- Genom ledningssystemet tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete
- Genom ledningssystemet tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver
- Genom ledningssystemet säkerställa att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas
- Upprätta en informationssäkerhetspolicy och andra styrande dokument,
- Informera medarbetare om krav på säker informationshantering och relevanta regler inom området
- Regelbundet, och enligt en beslutad utbildningsplan, genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas arbetsuppgifter
- Regelbundet, och enligt en beslutad övningsplan, genomföra övningar för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet
- Klassificera sin information med utgångspunkt i krav på konfidentialitet, tillförlitlighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd
- Identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster
- Utifrån informationsklassningens resultat och genomförd riskanalys identifiera och vidta de åtgärder som krävs för att uppfylla skyddsbehovet
- Följa upp och utvärdera vidtagna åtgärder och gjorda bedömningar av hot och risker
- Kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet
- Fortlöpande dokumentera vidtagna åtgärder
- 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

- Tillse att det finns rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott

Denna policy ersätter, av rektor den 23 december 2014, fastställd informationssäkerhetspolicy (Dnr: FS 1.1.2-1833-14).

Allmänt

Information är en av våra viktigaste tillgångar och utgör en förutsättning för att vi ska kunna bedriva vår verksamhet. Våra informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt med en helhetssyn på informationssäkerheten som inbegriper universitetets alla verksamhetsdelar. Detta då en säker informationshantering utgör en förutsättning för att vi skall kunna fullgöra uppdraget med att tillhandahålla utbildning, bedriva forskning samt att samverka med det omgivande samhället.

Informationssäkerhetsarbetet skall samordnas med övrigt säkerhetsarbete vid universitetet och de ledningssystem som antagits där.

Definitioner

Informationssäkerhet är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (ISO 27002.2.5). Informationssäkerheten avser såväl administrativ säkerhet som teknisk säkerhet

Informationstillgångar är allt som innehåller information och allt som bär på information. Till exempel information och informationsbehandlande system, programvara, fysiska tillgångar och hårdvara, tjänster, människor och immateriella tillgångar. (ISO 27002:7.1.1)

Konfidentialitet - Att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgänglig eller avslöjas för obehöriga

Tillgänglighet – Att informationstillgångar skall kunna utnyttjas i förväntad uträckning och inom önskad tid

Riktighet – Att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning

PDCA-modellen (”Plan-Do-Check-Act”). En strukturerad process för planering, genomförande, uppföljning och kontinuerlig förbättring som används i ISO’s (International Organization for Standardization) olika ledningssystem, känd och använd under sin engelska förkortning,

COSO-modellen (utvecklad av Committee of Sponsoring Organization). COSO-modellen består av fem delar: Kontrollmiljö, riskanalys, kontrollaktiviteter, information och kommunikation samt tillsyn. Därtill en riskvärdering utifrån sannolikhet och konsekvens med en skala på 1 till 4,

Med *hot* menas – möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten.

Målsättning

Målet för informationssäkerhetsarbetet vid Umeå universitet är att skydda dess informationstillgångar mot olika hot och att skapa en effektiv hantering och rutiner för att tillförsäkra att system och information omfattas av säkerhetsaspekterna konfidentialitet, tillgänglighet samt riktighet.

Roller och ansvar

Det övergripande ansvaret för myndigheten har *universitetsstyrelse* och *rektor*, vilket inbegriper ansvaret för universitetets informationssäkerhet. Rektor fastställer informationssäkerhetspolicy.

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.

Rektor utser en *informationssäkerhetsgrupp* som har till uppgift att utgöra ett rådgivande beredande organ till stöd för universitetsdirektörens informationssäkerhetsarbete, bland annat genom att tillse att ledningssystemet för informationssäkerhet vid Umeå universitet fungerar och efterlevs i dess olika delar. I detta organ ska följande funktioner finnas representerade:

IT-säkerhet, fysisk säkerhet, forskningsverksamhet, grundutbildning, administrativ verksamhet samt övriga funktioner som universitetsdirektören beslutar ingå.

Dekan respektive *prefekt/motsvarande* har ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerheten vid fakultet respektive institution/centrumbildning eller enhet.

För varje informationstillgång ska det finnas en *informationsägare* som ansvarar för alla delar av informationssäkerheten för informationstillgången. Informationsägaren ansvarar för informationstillgångens konfidentialitet, tillgänglighet och riktighet.

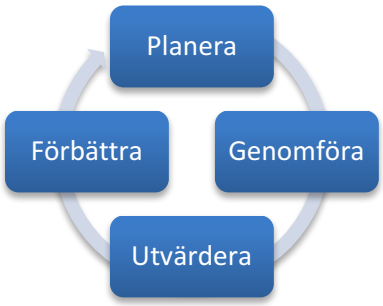
För information som ingår i IT-system gäller det ansvar och de roller som framgår av styrdokument för IT-verksamheten vid universitet såsom IT-säkerhetsplan, dnr 100-3305-10, och instruktion för systemförvaltning och systemägare.

Den som ingår avtal som leder till informationsanvändning eller informationsutbyte ansvarar för att kraven på informationssäkerhet specificeras i avtalet.

Arbetssätt

Ledningssystemet för informationssäkerhet vid Umeå universitet bygger på PDCA-modellen

enligt de övergripande stegen *Planera, Genomföra, Utvärdera* och *Förbättra*. Varje steg innehåller i sin tur en eller flera processer.[1]



PDCA modell fig 1

• **Planering** – Insamling av krav och målsättning samt framtagande av Risk- och sårbarhetsanalys.

Planeringsfasen omfattar bl. a. att årligen analysera gällande lagstiftning och gällande föreskrifter samt planera nästkommande års prioriterade arbete med informationssäkerhet. Här ingår översyn av risk- och sårbarhetsanalys. Arbetet sker på en universitetsövergripande nivå med stöd av en arbetsgrupp bestående av representanter för universitetsförvaltning och övrig verksamhet under ledning av informationssäkerhetsansvarig eller den till vilken denna delegerar uppgiften.

• **Genomföra** – Driva och genomföra det faktiska informationssäkerhetsarbetet.

Risk och sårbarhetsanalysen utgår från ovan nämnda kartläggning och klassificeras utifrån verksamhetsprocesser vilka följer Umeå universitets klassificeringsstruktur (Dnr FS 2.4.2.1-1910-14).

Klassificeringen sker därefter utifrån MSBs modell för klassificering av information med en bedömning av respektive process säkerhetsaspekt (*konfidentialitet, tillgänglighet samt riktighet)* samt konsekvensnivå enligt COSO-modellen.

Utifrån risk- och sårbarhetsanalysen upprättas inför varje år en handlingsplan som rektor fastställer. Handlingsplanen ska innehålla föreslagna åtgärder, status och ansvariga.

Anställda utbildas/informeras om informationssäkerhetsansvaret utifrån befattning och ansvar. Prefekter/motsvarande 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 genom att checklistan distribueras via nyhetsbrevet Nyheter för anställda.

[1] Processmodell baserad på metodstöd från www.informationssäkerhet.se

Kontinuitetsplaneringen består av en katastrofplan som gäller för centrala IT-resurser. I denna beskrivs de rutiner som finns för att IT-driften vid Umeå universitet ska kunna fungera vid en katastrof och om hur IT-driften ska kunna skötas från ett annat driftställe. Katastrofplanen är avsedd att användas i situationer som definierats som en katastrof, men ska även vara ett stöd i avbrottsplaneringen. Systemägaren ska ta fram en katastrofplan för varje system som den är ansvarig för. Hur detta ska göras beskriv i en framtagen mall. Krav på tillgänglighet för de centrala IT-resurserna har kartlagts och en prioritetslista har fastställts tillsammans med systemägarna.

Incidenthanteringen hanteras enligt fastställd process. Den anställde vänder sig till IRT (Incident Response Team). De ger råd och stöd kring olika typer av IT-säkerhetsincidenter, i allt från misstanke om konstig e-post, till misstanke om intrång av olika slag. Som stöd finns en mall för incidentrapportering och en mall för incidentanalys framtagna. En etablerad rutin finns fastställd för hur och när rapportering till MSB ska ske.

• **Utvärdera** - Mätning och uppföljning av krav och uppsatta mål för informationssäkerhetsarbetet.

En periodisk återkommande uppföljning av såväl föreliggande policy samt Risk och sårbarhetsanalys är viktig för att bevaka att ledningssystemet för informationssäkerhet vid Umeå universitet fungerar och efterlevs. I enlighet med rektors beslut om regelverk vid Umeå universitet ska policys följas upp fortlöpande och senast efter fem år genomgå en komplett översyn. Risk- och sårbarhetsanalys ska fastställas för en giltighet på tre år för att spegla förändringar och nya krav i verksamheten men kan revideras tidigare om behov föreligger.

Vid det årliga upprättandet av en handlingsplan för informationssäkerhetsarbetet görs en genomgång av risk- och sårbarhetsanalysen och vilka åtgärder som vidtagits under föregående år. Handlingsplanen fastställes av rektor. Därutöver sker en halvårsvis rapportering av informationssäkerhetsarbetet till universitetsdirektören.

Inom ramen för universitetets arbete med intern styrning och kontroll sker även en viss kontroll av informationssäkerhetsarbetet årligen. Inom detta arbete rapporteras inträffade incidenter genom avvikelserapportering.

• **Förbättra** – Resultat från uppföljningen ligger till underlag för kommande förbättringar och prioriteringar samt kompetensutveckling

Genom att kartlägga och systematisera universitetets informationssäkerhet enligt ovanstående modell kan hot och risker inom området kartläggas och eventuella åtgärder vidtas och föreliggande policys målsättning uppfyllas. Därför ska resultatet av risk- och sårbarhetsanalysen kommuniceras till berörda verksamheter. En generell information om LIS, inklusive bifogad checklista, som vänder sig till alla anställda och studenter ska även finnas tillgänglig via universitets hemsida för att öka medvetenheten om risker och hot inom området.

Bilagor

Risk- och sårbarhetsanalys