UPPSALA
UNIVERSITET

Dnr 2017/651

Systematiskt informationssäkerhetsarbete vid Uppsala universitet

---

Riktlinjer för säkerhetsarbetet vid Uppsala universitet

Fastställd av Säkerhetschefen 2016-04-16
Senast rev. 2022-03-17

Innehåll

1 Inledning

Informationssäkerhetsarbetet ska sträva efter **rätt säkerhet**, dvs. att balansera risker mot kostnader för skyddsåtgärder, och **styrd säkerhet**. Arbetet ska styras och utföras enligt detta dokument som är baserat på myndigheten för samhällsskydd och beredskaps (MSB) Metodstöd för systematiskt informationssäkerhetsarbete som i sin tur bygger på de internationella standarderna i ISO/IEC 27000-serien.

I underlaget till beslut och budget för universitetets informationssäkerhetsarbete ingår också arbete och uppföljning enligt *förordning om statliga myndigheters riskhantering* (SFS 1995:1300), samt universitetets årliga risk- och sårbarhetsanalys enligt MSBs föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7).

Arbetet med informationssäkerhet vid Uppsala universitet beskrivs enligt de sju avsnitten i ISO 27001:2017,

- Organisationens förutsättningar
- Ledarskap
- Planering
- Stöd
- Verksamhet
- Utvärdering av prestanda
- Förbättringar

och omfattas av säkerhetsåtgärder grupperade i enlighet med ISO 27002:2017,

- Informationssäkerhetspolicy
- Organisation av informationssäkerhetsarbetet
- Personalsäkerhet
- Hantering av tillgångar
- Styrning av åtkomst
- Kryptering
- Fysisk och miljörelaterad säkerhet
- Driftsäkerhet
- Kommunikationssäkerhet
- Anskaffning, utveckling och underhåll av system
- Leverantörsrelationer
- Hantering av informationssäkerhetsincidenter
- Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet
- Efterlevnad

Detta dokument, tidigare benämnt Ledningssystem för Informationssäkerhet (LIS), beskriver mål för vilka en balanserad säkerhetsnivå och lämpliga säkerhetsåtgärder ska planeras, genomföras, följas upp och kontinuerligt förbättras vid behov. Kontinuerlig uppföljning och förbättring, samt aktiv dialog med ledning och verksamhet är grundläggande för säkerhetsarbetet.

Fastställda styrdokument, riktlinjer, rutiner och andra stöddokument inom informationssäkerhet publiceras i universitetets mål- och regelsamling[1].

Nedan presenteras Uppsala universitets systematiska arbete med informationssäkerhet baserat på de sju avsnitten i SS-EN ISO/IEC 27001:2017.

2 Organisationens förutsättningar

Det övergripande målet för informationssäkerhetsarbetet är att upprätthålla en väl avvägd informationssäkerhet med hänsyn till universitetet, verksamma vid universitetet och allmänhetens behov i enlighet med uppdragen i Högskolelagen (SFS 1992:1434) om undervisning, forskning och samverkan med det omgivande samhället.

Informationssäkerhetsarbetet ska säkerställa att universitetets informationsresurser får ett adekvat, relevant och heltäckande skydd. I styrdokumentet *Rutiner för informationssäkerhet (UFV 2017/93)* anges de säkerhetskrav som ställs på universitetets informationssystem, såväl vid normal verksamhet som i tänkbara krissituationer.

3 Ledarskap

I universitets övergripande styrdokument *rutiner för informationssäkerhet (UFV 2017/93*) – motsvarande universitetets *informationssäkerhetspolicy* i enlighet med ISO 27001:2017 – beskrivs ansvar, roller och omfattning för arbetet med informationssäkerhet vid universitetet. Av denna rutin framgår att rektor har det övergripande ansvaret för verkställigheten av informationssäkerhetsarbetet, och ett kontrollansvar att utförandet följer det delegerade ansvaret.

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att informationssäkerhetsarbetet ska lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet.

Ledningen ska årligen, efter föredragning av CISO och säkerhetschef om informationssäkerhetsläget, fatta beslut om inriktningen för det fortsatta systematiska informationssäkerhetsarbetet.

4 Planering

Planering innebär ett strukturerat sätt att avgöra vilka risker och möjligheter som behöver hanteras för att dels förebygga eller minska oönskade effekter, dels uppnå ständig förbättring, och att planera åtgärder för att hantera dessa risker och möjligheter samt utvärdera åtgärdernas verkan.

[1] https://regler.uu.se/, 2021-03-23

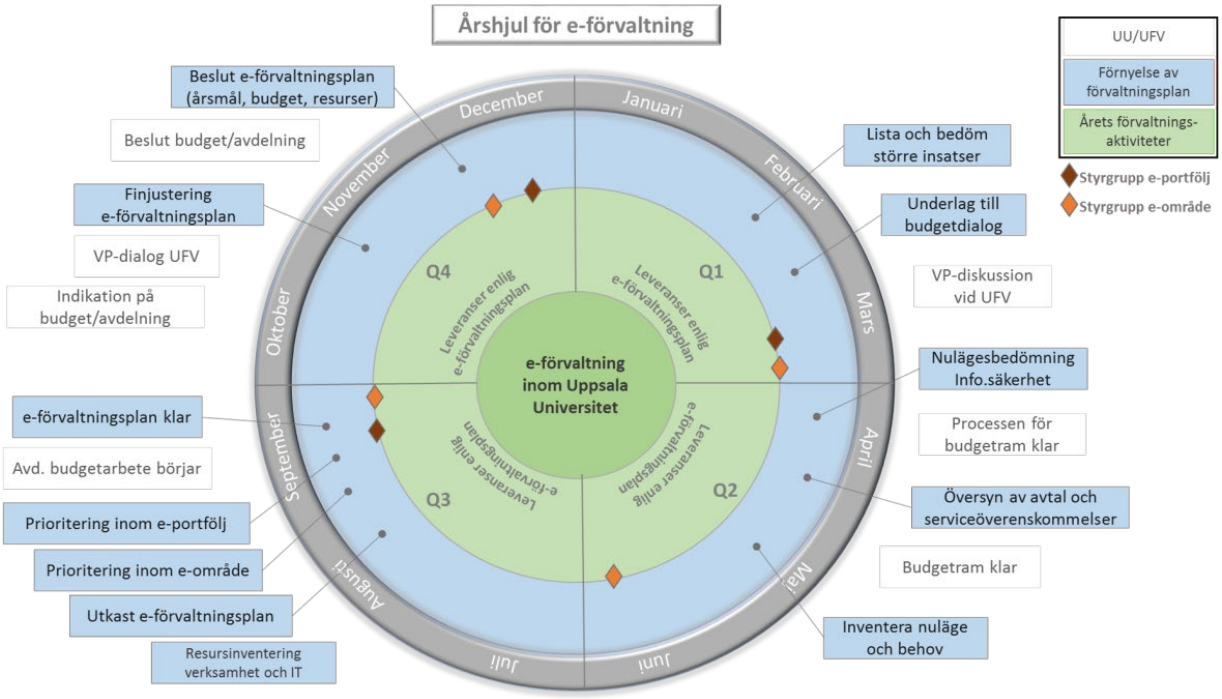
Planeringen ska baseras på *Rutiner för riskhantering (UFV 2018/211)*. Rutinerna ger ett verksamhetsanpassat stöd för kontinuerlig riskhantering av universitetets informationsresurser med avseende på konfidentialitet, riktighet och tillgänglighet.

Riskhanteringsprocessens ingående delar:

1. Avgränsning
2. Konsekvensanalys
3. Informationsklassificering
4. Kravanalys baserad på de 14 avsnitten i ISO 27002
5. Riskanalys
6. Hantering av identifierade säkerhetsbrister

Information om samtliga delar i riskhanteringsprocessen inklusive metodstöd finns beskrivet i *Rutiner för riskhantering (UFV 2018/211)*. Samtliga delar i processen ska dokumenteras vid genomförandet.

Riskhantering av universitetets centrala informationssystem är en integrerad del av universitetets systemförvaltningsmodell. Varje förvaltningsområde ansvarar för ett löpande arbete med informationssäkerheten för de system som ingår i det egna området. Informationsklassificering och kravanalyser ska upprättas och underhållas för varje system. En riskbedömning av ej uppfyllda krav ska genomföras som en del av förvaltningsområdenas informationssäkerhetsarbete. Denna riskbedömning ska ligga till grund för prioriteringar och beslut om förbättringar att ta upp i förvaltningsplan och budget för nästkommande verksamhetsår.
Ett särskilt moment benämnt nulägesbedömning ska äga rum en gång per år för uppföljning och prioritering av eventuella åtgärder. Informationssäkerhetsarbetet har integrerats i det årshjul som anger hur förvaltningsarbetet ska bedrivas, se bild nedan.



Universitetets säkerhetsavdelning bidrar med stöd i det lokala arbetet med riskhantering vid institutioner och intendenturer.

5 Stöd

Stödet för universitetets informationssäkerhetsarbete fördelar sig på resurser och kompetens, medvetandegörande av verksamma, kommunikation och dokumenterad information. Resurser för att underhålla och ständigt förbättra informationssäkerhetsarbetet hanteras av universitetets säkerhetsavdelning.

Grundläggande utbildningar i informationssäkerhet erbjuds både via lärarledda tillfällen och via internetbaserade kurser. Utöver detta erbjuds målgruppsanpassade kurser och informationsträffar enligt behov och önskemål. För ytterligare stöd finns möjlighet att kontakta universitetets säkerhetsavdelning. Kommunikation med verksamma sker även via e-postlistor, olika forum, personalmöten med mera.

Information, länkar till riktlinjer och rutiner samt vägledning i säker informationshantering finns tillgängligt på särskild plats i universitetets medarbetarportal. Riktlinjer och rutiner inom informationssäkerhetsområdet finns i universitetets mål- och regelsamling.

6 Verksamhet

Uppsala universitet ska planera, införa och styra de processer som krävs för att uppfylla informationssäkerhetskraven och införa åtgärderna som fastställs i riskhanteringsprocessen. Därtill ska organisationen införa planer för att uppnå fastställda informationssäkerhetsmål.

E-områdenas informationsarbete ska dokumenteras i särskilda ytor i organisationens Wiki. Resultat för genomförda informationsklassificeringar och kravanalyser i övriga delar av verksamheten ska tillsändas säkerhetsavdelningen.

Informationssäkerhetskraven identifieras med hjälp av olika åtgärder som t.ex. härledning från författningar och interna regelverk, riskanalyser, analys av incidenter och resultat från genomförda informationsklassificeringar.

7 Utvärdering av prestanda

Periodisk uppföljning och rapportering av hur säkerhetsarbetet fungerar i verksamheten med avseende på uppsatta mål, praktisk erfarenhet och efterlevnad utförs i huvudsak av universitetets säkerhetsavdelning.

Säkerhetschefen rapporterar till universitetsledningen regelbundet.

I universitetets årliga risk- och sårbarhetsanalys finns sammanställningar av det som genomförts inom ramen för systematiskt informationssäkerhetsarbete. Dessa sammanställningar inkluderar analys av riskområden tillsammans med förbättringsförslag.

Inom säkerhetsavdelningens ansvarsområde ingår sammanställning och uppföljning av informationssäkerhetsincidenter, resultat av genomförda riskanalyser, resultat av interna eller externa IT-revisioner, samt konsekvenser av eventuella förändringar i tillämpliga lagar, föreskrifter eller avtalsförpliktelser.

8 Förbättringar

Ständiga förbättringar av universitetets systematiska informationssäkerhetsarbete med avseende på funktionalitet och kvalitet uppnås genom

- korrigerande och förebyggande åtgärder
- information och utbildning
- omvärldsbevakning

Förslag och prioriteringar av förbättringar i det systematiska informationssäkerhetsarbetet ska ingå som en del av säkerhetschefens löpande planering och uppföljning samt utgöra underlag för den årliga verksamhetsplanen för avdelningen.

För respektive e-område eller för ett enskilt informationssystem ska förslag och prioriteringar av förbättringsåtgärder ingå i det ordinarie förvaltningsarbetet samt utgöra underlag för den årliga förvaltningsplanen.

Planer för behandling av risker genom olika åtgärder ska följas upp löpande.