Mittuniversitetet
MID SWEDEN UNIVERSITY

Riktlinjer för informationssäkerhet

Publicerad: 2021-05-04

Beslutsfattare: Lotten Glans

Handläggare: Eva Rodin Svantesson

Beslutsdatum: 2021-05-04

Giltighetstid: Tillsvidare

Sammanfattning: Riktlinjerna för informationssäkerhet är ett av styrdokumenten i Mittuniversitetets LIS. Riktlinjerna beskriver de sju avsnitten i ISO 27001:2017 och de grupper som omfattas av säkerhetsåtgärder enligt ISO 27002:2017. Riktlinjerna har anpassats utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

Tidigare versioner:
Dnr MIUN 2019/1629, 2019-10-01

Innehållsförteckning

1. Inledning

Det övergripande målet för informationssäkerhetsarbetet är att upprätthålla en väl avvägd informationssäkerhet med hänsyn till universitetet, verksamma vid universitetet och allmänhetens behov. Informationssäkerhetsarbetet ska sträva efter *Rätt säkerhet*, dvs. att balansera risker mot kostnader för skyddsåtgärder, och *Styrd säkerhet*, dvs. styras och utföras enligt Mittuniversitets ledningssystem för informationssäkerhet, LIS. Ett fungerande LIS är ett led i att säkerställa att universitetets informationsresurser får ett heltäckande och adekvat skydd.

Enligt Myndigheten för samhällsskydd och beredskaps föreskrift om informationssäkerhet för statliga myndigheter (MSBF:S 2020:6) ska myndigheten bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna *SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav* och *SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder* eller motsvarande.

2. Organisationens förutsättningar

Organisationens förutsättningar (förstå organisationen, intressenter och dess förutsättningar, bestämma omfattningen av LIS)

Arbetet med LIS vid Mittuniversitet beskrivs enligt de sju avsnitten i ISO 27001:2017 och omfattas av säkerhetsåtgärder grupperade under fjorton rubriker i 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

LIS beskriver säkerhetsmål för vilka en balanserad säkerhetsnivå och lämpliga säkerhetsåtgärder ska planeras, genomföras, följas upp och kontinuerligt förbättras vid behov.

Grundläggande för IT- och informationssäkerhetsarbetet är kontinuerlig uppföljning och förbättring, ofta beskrivet genom den s.k. PDCA-cykeln ("Plan-Do-Check-Act"), samt aktiv dialog med ledning och verksamhet.

Föreskrifter och vägledningar som berör informationssäkerhet:

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2020:6
- Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, MSBFS 2020:7
- Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter, MSBFS 2020:8
- Myndigheten för samhällsskydd och beredskaps vägledning - säkerhetsåtgärder i informationssystem för statliga myndigheter

Som stöd i det dagliga arbetet finns det policydokument, riktlinjer, rutiner och andra stöddokument inom informationssäkerhet fastställda och publicerade på medarbetarsidorna. Nya dokument tas fram vid behov och befintliga ses över kontinuerligt.

3. Ledarskap

Ledarskap och engagemang, policy, befattningar, ansvar

- Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret; från ledning ner till enskilda medarbetare.
- Varje medarbetare ska aktivt arbeta för ökad säkerhet, samt påpeka brister till överordnad.
- Enligt Mittuniversitetets systemförvaltningsmodell ansvarar systemägarna för informationssäkerheten kring verksamhetssystemen.
- Dataskyddsombudets ansvar framgår av MIUN 2018/713
- Ansvaret för informationssäkerhetsarbetet finns hos INFRA-avdelningen enligt beslut av rektor MIUN 2019/583. I ansvaret ingår att besluta om riktlinjer, rutiner, processer etc. samt se till att ett aktivt arbete bedrivs kring frågorna, inklusive att ta fram ett LIS. För arbetet ska det finnas en informationssäkerhetssamordnare.

Som stöd i informationssäkerhetsarbetet finns funktioner för arkiv, juridik och dataskydd.

4. Planering

Planering (Åtgärder för att hantera risker och möjligheter, bedömning och behandling av informationssäkerhetsrisker, informationssäkerhetsmål)

Planering innefattar åtgärder för att hantera risker och möjligheter, bedömning och behandling av informationssäkerhetsrisker samt informationssäkerhetsmål. Detta processteg innebär att planera för och följa upp införandet av LIS samt löpande förbättringsåtgärder. Planeringen och uppföljningen ska vara baserade på framtagna anvisningar (se medarbetarsidorna).

Riskhantering av universitetets centrala system är en integrerad del av universitetets systemförvaltningsmodell. Detta innebär att varje systemgrupp ska genomföra en s.k. analys av informationssäkerheten en gång per år (i samband med framtagandet av förvaltningsplanen). Analysen ligger sedan som

underlag för prioriteringar och beslut om förbättringar och budget för nästkommande verksamhetsår.

Informationssäkerhetsarbetet integreras i ett årshjul som anger hur arbetet ska bedrivas, se bild nedan.

För kärnverksamheten sker motsvarande genom arbete och uppföljning enligt föreskriften om statliga myndigheters riskhantering och föreskriften om statliga myndigheters informationssäkerhet. Underlaget är avgränsat till frågor kring förebyggande och avhjälpande risk- och skadehantering samt säkerhetsrelaterade och informationssäkerhetsrelaterade frågor, tillsammans med frågor rörande andra lagrum inom samma eller liknande ämnesområden. Underlaget inhämtas från universitetets alla institutioner och avdelningar på förvaltningen.

5. Stöd

Stöd (resurser, information, kompetens)

Avdelningen för infrastruktur ansvarar för att aktuell och lättillgänglig information om riktlinjerna för informationssäkerhet finns tillgängliga på universitetets webbplats.

Informations- och utbildningsinsatser om informationssäkerhetsarbetet ska kunna erbjudas vid respektive institution/motsvarande. Grundläggande utbildningar erbjuds på olika sätt, både generella och mer målgruppsanpassade enligt behov och önskemål. Detta sker dels genom utbildningar som vänder sig till flera anställda samtidigt och dels genom medarbetarens ansvar för sin egen kompetensutveckling, som lyfts årligen vid medarbetarsamtalen.

6. Verksamhet

Verksamhet (planering och styrning av verksamheten, samt bedömning och behandling av informationssäkerhetsrisker)

Planering och styrning av verksamheten samt bedömning och behandling av informationssäkerhetsrisker är en central del i LIS.
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.

Rutinerna och processerna för riskanalyser av informationssystem, beskriver universitetets process för genomförande av informationsklassificering. Stöddokument för momenten finns på medarbetarsidorna.

7. Utvärdering av prestanda

Utvärdering av prestanda (övervakning mätning, analys och utvärdering, internrevision, ledningens genomgång)

Universitetet ska utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärdering av prestanda sker genom

övervakning, mätning, analys och utvärdering, internrevision, ledningens genomgång m.m. Periodisk uppföljning och rapportering av hur säkerhetsarbetet fungerar i verksamheten med avseende på uppsatta mål, praktisk erfarenhet och efterlevnad utförs i huvudsak av avdelningen för infrastruktur.

Informationssäkerhetsarbetet redovisas för ledningsrådet 2 ggr/år och innehåller följande information:

- Utvärderingar av interna regler, arbetssätt och stöd
- Informationsklassningar
- Riskbedömningar
- Utvärderingar av säkerhetsåtgärder
- Utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt
- I vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov
- Allvarliga risker som inte har åtgärdats
- Övriga hinder (bör inkludera brister avseende tilldelning av ansvar, resurser, mandat och befogenheter samt brister avseende interna regler och arbetssätt) för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet

8. Förbättringar

Förbättringar (Avvikelse och korrigerande åtgärd, ständig förbättring)

Ständiga förbättringar av LIS med avseende på funktionalitet och kvalitet uppnås genom:

- korrigerande och förebyggande åtgärder
- information och utbildning
- omvärldsbevakning

Förslag och prioriteringar av förbättringar i LIS ska ingå som en del av avdelningen för infrastrukturs löpande planering och uppföljning av

informationssäkerhetsarbetet samt utgöra underlag för den årliga verksamhetsplanen.

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

Det årliga arbetet med riskhantering ur ett säkerhetsperspektiv i kärnverksamheten kan följas upp genom besök vid institutioner utifrån identifierade behov.