# **Checklista för nulägesbedömning av informationssäkerheten i ett e-område, enskilt informationssystem eller grupp av system med likartade säkerhetskrav.**

##

Nedanstående checklista är avsedd att vara ett stöd till universitetets förvaltningsorganisation i informationssäkerhetsarbetet.

Informationssäkerhetsarbetet ska säkerställa att risker, störningar och hot mot universitetets informationsresurser identifieras och hanteras så att negativa konsekvenser avseende *tillgänglighet*, *riktighet* och *konfidentialitet* minimeras.

Bedöm efterlevnad av nedanstående punkter, baserade på svensk standard SS-ISO/IEC 27001:2014 och SS-ISO/IEC 27002:2014 samt universitetets riktlinjer för informationssäkerhet. Ange grad av efterlevnad för respektive punkt enligt skalan nedan.

2 = God efterlevnad

1 = Bristfällig efterlevnad

0 = ingen efterlevnad

Et = Ej tillämpligt

# **Särskilda skyddsåtgärder för system som klassificeras som skyddsvärda och/eller verksamhetskritiska.**

Särskilda skyddsåtgärder för system som hanterar information som klassificeraras som **Hög nivå** eller **Särskilda krav** avseende **Konfidentialitet** (Skyddsvärda) respektive **Tillgänglighet och Avbrottskydd** (Verksamhetskritiska). (*Bilaga 1a till Riktlinjer för riskhantering av informationssystem).*

 *Markerar prioriterade skyddsåtgärder för system som klassificeras som skyddsvärda.*

 *Markerar prioriterade skyddsåtgärder för system som klassificeras som verksamhetskritiska.*

**Skyddsvärda system** är system som omfattas av lagar och förordningar som OSL och PUL och därför behöver ett starkt skydd mot att informationen görs tillgänglig för obehöriga personer, system eller processer för att motverka möjliga konsekvenser som skulle kunna bli mycket allvarliga för enskilda personer, universitetet eller tredje part.

Exempel på skyddsvärda system i universitetets verksamhet är system som hanterar skyddade identiteter och adresser, sekretesskyddad information, starkt integritetskänslig information (t.ex. sjukdomsuppgifter), särskilt känslig forskningsinformation (företagshemligheter), ritningar över lokaler där känslig verksamhet bedrivs eller värdefulla tillgångar förvaras, upphandlingsinformation etc.

**Verksamhetskritiska system** är system eller IT-tjänster som är av mycket stor betydelse för universitetets kärnverksamhet och därför behöver ett skydd som möjliggör att informationen är åtkomlig och användbar på förväntat sätt och inom önskad tid för att motverka möjliga konsekvenser som skulle kunna få mycket allvarliga konsekvenser för enskilda personer, universitetet eller tredje part.

Exempel på verksamhetskritiska system universitetets externa webbsidor, Outlook för e-post och kalender, de delar av Studentportalen som studenter behöver för att fullgöra sina studier (tider, lokaler etc.) samt katalog- och inloggningstjänster (DNS, DHCP, CAS, AKKA etc) och andra gemensamma tjänster som är av mycket stor betydelse för utnyttjandet av samtliga IT-tjänster på universitetet.

|  |  |  |  |
| --- | --- | --- | --- |
| *Nr.* | *Att bedöma – gå igenom punkt för punkt nedan* | *0, 1, 2, Et* | *Plats för noteringar* |

1. **Riktlinjer**

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1 | e-områdesansvariga och e-koordinatorer (systemägare och systemansvariga) ska känna till var riktlinjer för informationssäkerhet finns med underliggande riktlinjer, anvisningar och stöddokument. |  |  |

1. **Organisation och ansvar**

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1 | e-områdesansvariga (systemägare) ska vara införstådda med sitt ansvar för informationssäkerheten i berörda system och arbeta aktivt med att initiera, stödja och följa upp säkerhetsförbättringar.  |  |  |
| 2.2 | e-koordinatorer (systemansvariga) ska vara införstådda med sitt ansvar att koordinera och driva arbetet med informationssäkerhet. |  |  |
| 2.3 | Ansvar och ansvarsområden i förvaltningsorganisationen som kan stå i konflikt med varandra och därmed äventyra informationssäkerheten ska separeras. *Exempel på detta kan vara personer som både kan föreslå, besluta om och införa ändringar.*  |  |  |
| 2.4 | Förvaltningsorganisationen ska via medarbetarportalen ta del av aktuell säkerhetsrelaterad information (ex. Ledningsnytt, säkforum, driftinformation). |  |  |
| 2.5 | Förvaltningsorganisationen ska känna till att IT- och informationssäkerhetsincidenter ska anmälas till servicedesk. |  |  |

1. **Personal**

|  |  |  |  |
| --- | --- | --- | --- |
| 3.1 | Användare av system som inte använder gemensam webbinloggning ska känna till Allmänna regler för användning av användarkonton och datornät (Dnr UFV 2013/1502) och att disciplinära eller rättsliga åtgärder kan vidtas vid överträdelse. Not. För system som använder gemensam webbinloggning hanteras detta automatiskt. |  |  |
| 3.2 | Användare av system bör ha genomgått säkerhetsavdelningens webbaserade kurs i informationssäkerhet:<https://mp.uu.se/web/info/anstallning/kompetensutveckling/intern/sakerhet>  |  |  |
| 3.3 | Systemanvändare med höga behörigheter eller som har tillgång till känslig information ska ha gått någon av säkerhetsavdelningens lärarledda kurser i informationssäkerhet. |  |  |
| 3.4 | Bakgrundskontroll ska göras av sökande till anställning som innebär tillgång till särskilt känslig information. |  |  |
| 3.5 | En dokumenterad och godkänd rutin för återlämning eller annan avtalad hantering av datorer, mobila enheter, datamedia etc. ska finnas och följas vid avslut eller ändring av anställning. |  |  |

1. **Tillgångar**

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1 | e-områdets Förvaltningsplan ska tydligt ange vilka informationsresurser (system, hård- och mjukvara, databaser eller på annat sätt lagrad information, kommunikationslösningar) som ingår i e-området. |  |  |
| 4.2 | Den information som tillhör e-området ska vara klassificerad enligt universitetets Riktlinjer för riskanalyser av informationssystem. |  |  |
| 4.3 | Register som innehåller personuppgifter ska vara anmälda till universitetets personuppgiftsombud vid juridiska avdelningen. |  |  |

1. **Åtkomst**

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1 | Alla system bör vara kopplade till universitetets gemensamma inloggningstjänst. |  |  |
| 5.2 | En dokumenterad rutin för behörighetstilldelning ska finnas och följas. Denna rutin ska omfatta samtliga förekommande behörighetsnivåer. |  |  |
| 5.3 | Alla användare av systemet/systemen ska ha en unik användaridentitet, dvs. inga gruppidentiteter får finnas. |  |  |
| 5.4 | Rutinerna ska ange att tilldelning av sysadmin- och användarkonton med höga behörigheter ska begränsas samt granskas och revideras regelbundet. Dessa ska omfatta att medge, förändra och återkalla åtkomst till information, system och tjänster. |  |  |
| 5.5 | För att reducera risken för obehörig åtkomst ska* systemfunktion som kopplar ner sessionen efter en fastställd tidsperiod av inaktivitet finnas
* systemanvändare som har tillgång till känslig information ha en tidsstyrd skärmsläckare installerad på sina datorer
 |  |  |
| 5.6 | Programvaruleverantörers och annan servicepersonals åtkomst till känslig information ska begränsas och vara reglerad i sekretessavtal.  |  |  |
| 5.7 | Lösenord ska vara utformade, hanteras och användas i enlighet med de riktlinjer för lösenord som gäller vid universitetet. |  |  |
| 5.8 | Det ska gå att begränsa användares åtkomst till system och databaser utifrån roll, organisationstillhörighet etc. |  |  |
| 5.9 | Alla användare ska vara medvetna om det personliga ansvaret för att skydda sina lösenord till systemet/systemen. |  |  |
| 5.10 | Om åtkomst till system innehållande känslig information sker på distans ska universitetets VPN-tjänster för säker internetuppkoppling användas. |  |  |
| 5.11 | Åtkomst till tjänster och verktyg (operativsystem, nätverkstjänster, systemverktyg etc.) med möjlig påverkan på systemets/systemens säkerhet ska begränsas och styras strikt. |  |  |
| 5.12 | Användning av verktyg (t.ex. SQL-verktyg) som kan kringgå säkerhets- och loggningsåtgärder i systemet/systemen ska begränsas och styras strikt, exempelvis genom användning av manuell logg. |  |  |
| 5.13 | Tvåfaktorautentisering för förhöjd inloggningssäkerhet bör införas för system innehållande känslig information.  |  |  |
| 5.14 | Särskilda ansvarsförbindelser som tydligt reglerar systemadministratörers och användares med höga behörigheter/rättigheter och skyldigheter bör införas. |  |  |

1. **Kryptering**

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1 | Om systemet hanterar information med höga eller särskilda krav på sekretess ska databaser och datakommunikation vara krypterade. |  |  |

1. **Fysisk och miljörelaterad säkerhet (Teknik med fokus på driftmiljö).**

|  |  |  |  |
| --- | --- | --- | --- |
| 7.1 | Lokaler där systemets/systemens datordrift sker eller där datamedia förvaras ska vara skyddade med ett ändamålsenligt skalskydd - lås, larm, passagesystem (kort och kod) etc. för att minimera risken för obehörig åtkomst. Särskilda skyddsåtgärder ska övervägas för lokaler som innehåller känslig eller kritisk information eller utrustning. |  |  |
| 7.2 | Endast behörig personal ska ha tillträde till berörda lokaler eller utrymmen för systemet/systemen. Dokumenterade rutiner ska finnas och följas för tillträde till och arbete i berörda lokaler. |  |  |
| 7.3 | Systemets/systemens datorutrustning ska vara placerade och skyddade på ett sådant sätt att riskerna för miljörelaterade hot (temperatur, brand, vatten) minimeras. |  |  |
| 7.4 | Systemets/systemens fysiska utrustning (hårddiskar, kablar, fläktar etc.) ska underhållas och uppdateras på ett korrekt sätt som säkerställer fortsatt tillgänglighet och riktighet. |  |  |
| 7.5 | När utrustning som kan innehålla skyddsvärd information ska flytta mellan användare inom eller mellan institutioner, eller ska avvecklas eller avyttras (kasseras, bytas bort eller försäljas) ska universitetets riktlinjer för hantering av utrangerad IT-utrustning följas. |  |  |
| 7.6 |  | Om systemet/systemen har höga eller särskilda krav på tillgänglighet ska avbrottsfri kraft (UPS) för datordriften finnas installerad hos driftsleverantören som även ska kunna uppvisa rutiner och dokumentation av att regelbundna tester av UPS-systemet genomförs. |  |  |
| 7.7 | Dokumenterade regler och rutiner ska finnas för fysisk transport av data, exempelvis via portabla lagringsmedia som USB-minnen och liknande. |  |  |

1. **Driftsäkerhet (Teknik med fokus på driftmiljö).**

|  |  |  |  |
| --- | --- | --- | --- |
| 8.1 | En formaliserad ändringshanteringsprocess (ex.vis change management där ITIL tillämpas) avseende nya versioner av aktuella tjänster, hårdvara, systemprogramvara och operativsystem ska finnas och tillämpas av driftsleverantören. |  |  |
| 8.2 | En formaliserad problem- och incidenthanteringsrutin ska tillämpas av driftsleverantören. |  |  |
| 8.3 | Utvecklings-, test- och produktionsmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljöer. |  |  |
| 8.4 | Om systemet har höga eller särskilda krav på tillgänglighet ska driftsleverantören dagligen övervaka och vid behov justera kapacitetsbehovet samt även göra regelbundna prognoser av framtida kapacitetskrav. |  |  |
| 8.5 | Säkerhetskopior av systemets/systemens databaser, programvara och övriga kritiska funktioner eller parametrar ska tas och testas regelbundet. |  |  |
| 8.6 | Användaraktiviteter i systemet/systemen ska loggas och loggarna ska sparas på ett säkert sätt enligt universitetets riktlinjer för loggning. |  |  |
| 8.7 | Systemoperatörers och administratörers aktiviteter i systemet/systemen ska loggas och loggarna ska sparas på ett säkert sätt enligt universitetets riktlinjer för loggning. |  |  |
| 8.8 | Loggar och loggningsverktyg ska vara skyddade mot obehörig åtkomst och manipulation. |  |  |
| 8.9 | Systemet/systemen ska vara anslutet till en central systemklocka (NTP) för synkronisering mot en och samma referenskälla för tid. Universitetets centrala tidsservrar ska användas av de system som är anslutna till universitetets nätverk. |  |  |
| 8.10 | Fysiskt separerade databaser och nätverksegmentering för lagring respektive kommunikation av känslig information ska övervägas. |  |  |

1. **Kommunikationssäkerhet (Teknik med fokus på driftmiljö).**

|  |  |  |  |
| --- | --- | --- | --- |
| 9.1 | De nätverk som systemet/systemen använder för dataöverföring ska vara uppbyggda, administrerade och övervakade av driftsleverantören på ett sätt som säkerställer tillräcklig säkerhet. |  |  |
| 9.2 | Säkerhetsåtgärder som uppfyller systemets/systemens krav på säker dataöverföring i de nätverkstjänster som används ska vara överenskomna och specificerade i avtal med driftsleverantören. |  |  |
| 9.3 | Känslig information i systemet/systemen får inte distribueras via okrypterad e-post, sociala medier, molntjänster etc. |  |  |
| 9.4 | Vid överföring av känslig information till annat system inom universitetet ska motsvarande skyddsåtgärder som inom det egna systemet/systemen vara vidtagna. |  |  |
| 9.5 | Vid överföring av känslig information till annan myndighet ska motsvarande skyddsåtgärder som på Uppsala universitet vara vidtagna. |  |  |
| 9.6 | Vid överföring av känslig information till andra externa parter ska skyddsåtgärder vid bearbetning, lagring och publicering av informationen vara reglerade i avtal. |  |  |

1. **Anskaffning, utveckling och underhåll**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10.1 |  | En dokumenterad mottagningsprocess ska användas då nya system eller tjänster knyts till e-området. Denna process ska inkludera nedanstående för att säkerställa att även tillkommande system/tjänster uppfyller gällande krav på informationssäkerhet.* En riskanalys ska genomföras för att bedöma potentiella säkerhetsrisker.
* En åtgärdsplan för att förbygga ovan identifierade säkerhetsrisker ska upprättas (resultat från riskanalys).
* Universitetets riktlinjer för anskaffning och drift av IT-system ska beaktas.
 |  |  |
| 10.2 | Allt arbete med utveckling och underhåll ska utföras i enlighet med universitetets riktlinjer för säker systemutveckling. |  |  |
| 10.3 | Systemet/systemen ska vara utformat i enlighet med kraven i offentlighets- och sekretesslagen (OSL) och personuppgiftslagen (PUL). Om osäkerhet råder ska universitetets säkerhetsavdelning eller juridiska avdelning tillfrågas. |  |  |

1. **Leverantörsrelationer**

|  |  |  |  |
| --- | --- | --- | --- |
| 11.1 | Om systemet/systemen hanterar känslig information ska en riskbedömning göras innan leverantörer eller andra externa parter ges tillgång till denna. |  |  |
| 11.2 | Relevanta informationssäkerhetskrav vara fastställda i avtal med alla leverantörer till systemet/systemen. I detta avtal ska även ett sekretessavtal ingå. |  |  |
| 11.3 | All personal som hyrs in från leverantörer till systemet/systemen ska vara informerade om de säkerhets- och sekretesskrav som har avtalats. |  |  |
| 11.4 | Regelbundna uppföljnings- och planeringsmöten med leverantörer till systemet/systemen ska genomföras. |  |  |
| 11.5 | Ändringar med avseende på verksamhets- eller säkerhetskrav i avtalade leverantörstjänster ska hanteras enligt en överenskommen rutin. Översyn och eventuell revison av gällande avtal ska göras |  |  |

1. **Incidenthantering**

|  |  |  |  |
| --- | --- | --- | --- |
| 12.1 | Säkerhetsincidenter och säkerhetsbrister ska anmälas till servicedesk.  |  |  |
| 12.2 | Systemets/systemens förvaltningsorganisation ska följa upp inrapporterade säkerhetsincidenter och -brister som avseende på vilka avhjälpande och/eller förebyggande åtgärder som har vidtagits. |  |  |

1. **Kontinuitet**

|  |  |  |  |
| --- | --- | --- | --- |
| 13.1 | Systemets/systemens återstartskrav ska vara avtalade med driftsleverantören i SLA eller motsvarande. |  |  |
| 13.2 | Återläsning av backup ska testas enligt avtalad periodicitet. |  |  |
| 13.3 | En reservrutin/kontinuitetsplan ska upprättas för att säkerställa att berörd verksamhet kan bedrivas även under ett långvarigt avbrott i ordinarie drift av systemet/systemen. Reservrutin/kontinuitetsplanen ska uppdateras löpande och testas vid behov eller enligt avtalad periodicitet. |  |  |
| 13.4 | Om (manuella) reservrutiner i verksamheten finns ska även dessa ses över (och testas) på regelbunden basis och/eller vid behov. |  |  |
| 13.5 | En strategi för att undvika nyckelpersonsberoende bör övervägas. |  |  |

1. **Efterlevnad**

|  |  |  |  |
| --- | --- | --- | --- |
| 14.1 | Känsliga personuppgifter ska hanteras i enlighet med personuppgiftslagen (PUL) och vara skyddade med lämpliga tekniska och organisatoriska åtgärder. |  |  |
| 14.2 | Uppgifter som skyddas av sekretess ska hanteras enligt offentlighets- och sekretesslagen (OSL) och ska vara skyddade med lämpliga tekniska och organisatoriska åtgärder. |  |  |

## Koppling till svensk standard SS-ISO/IEC 27001:2014 och SS-ISO/IEC 27002:2014

Nedan visas hur respektive punkt (1-14) i nulägesbedömningen mappar mot avsnitt i SS-ISO/IEC 27001:2014 och SS-ISO/IEC 27002:2014.

För åtgärdsmål och säkerhetsåtgärder – se SS-ISO/IEC 27001:2014, Bilaga A samt SS-ISO/IEC 27002:2014, kapitel 5 – 18.

**Avsnitt i nulägesbedömning Avsnitt i SS-ISO/IEC 27001:2014 och SS-ISO/IEC 27002:2014**

|  |  |
| --- | --- |
| 1. Riktlinjer
 | 5. Informationssäkerhetspolicy |
| 1. Organisation och ansvar
 | 6. Organisation av informationssäkerhetsarbetet |
| 1. Personal
 | 7. Personalsäkerhet |
| 1. Tillgångar
 | 8. Hantering av tillgångar |
| 1. Åtkomst
 | 9. Styrning av åtkomst |
| 1. Kryptering
 | 10. Kryptering |
| 1. Fysisk och miljörelaterad säkerhet (Teknik med fokus på driftmiljö)
 | 11. Fysisk och miljörelaterad säkerhet |
| 1. Driftsäkerhet (Teknik med fokus på driftmiljö)
 | 12. Driftsäkerhet |
| 1. Kommunikationssäkerhet (Teknik med fokus på driftmiljö)
 | 13. Kommunikationssäkerhet |
| 1. Anskaffning, utveckling och underhåll
 | 14. Anskaffning, utveckling och underhåll av system |
| 1. Leverantörsrelationer
 | 15. Leverantörsrelationer |
| 1. Incidenthantering
 | 16. Hantering av informationssäkerhetsincidenter |
| 1. Kontinuitet
 | 17. Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet |
| 1. Efterlevnad
 | 18. Efterlevnad |