HÖGSKOLAN
DALARNA

Plan för informationssäkerhet vid Högskolan Dalarna

2015

Beslut: 2015-05-04
Reviderad:
Dnr: DUC 2015/769/10
Ersätter:
Relaterade dokument: Policy för informationssäkerhet
Ansvarig: Förvaltningschef

Innehållsförteckning

1 Inledning

Till följd av den ständigt ökande utvecklingen och användningen av informationsteknik och nätbaserade informationstjänster utsätts högskolans informationsresurser för både ett växande antal hot och en större bredd av desamma, vilket medför en risk för ökad sårbarhet.

Denna plan beskriver införandet av Högskolan Dalarnas ledningssystem för informationssäkerhet (LIS) som är baserat på svensk standard SS-ISO/IEC 27001 och Policy för informationssäkerhet, DUC 2014/2174/10. MSB:s föreskrift anger att samtliga svenska myndigheter ska tillämpa ett ledningssystem för informationssäkerhet, MSBFS 2009:10.

Syftet med planen är att den ska utgöra en grund för informationssäkerhetsarbetet vid högskolan samt ge en övergripande beskrivning av de säkerhetskrav som ställs på våra informationssystem, såväl vid normal verksamhet som i tänkbara krissituationer.

2 Ansvar och organisation

Ansvaret för informationssäkerhet och efterlevnad av högskolans Plan för informationssäkerhet följer linjeorganisationen samt delegationsordningen och fördelar sig enligt följande:

- *Rektor* har övergripande ansvar
- *Akademichef/motsvarande* har ansvaret vid sin akademi/avdelning, i enlighet med högskolans delegationsordning
- *Informationssäkerhetsansvarig* ansvarar för implementering av ledningssystem för informationssäkerhet (LIS) och även planering, samordning, uppföljning och kontroll av efterlevnad
- *Systemägare/förvaltningsobjektägare* har vid sidan av ovanstående befattningar ansvaret för implementering och efterlevnad av plan inom sitt informationssystem/förvaltningsobjekt, inklusive där ingående informationsresurser.
- *Verksamma vid högskolan* ansvarar för att följa styrande dokument avseende informationssäkerhet vid egen användning av högskolans informationsresurser.

2.1 Ansvar för externa parter vid högskolan

Ansvar för externa parter (exempelvis konsulter och leverantörer) avseende tillgång till högskolans informationsresurser (utnyttjande, förvaltning, underhåll, utveckling etc.) ska vid behov tydligt regleras i avtal.

3 Definitioner

Informationsresurser innefattar all elektronisk, pappersbaserad, muntlig eller på annat sätt lagrad eller kommunicerad information samt de *informationssystem* (hård- och mjukvara) och kommunikationslösningar som hanterar informationen.

Informationssäkerhet syftar till att upprätthålla önskad nivå av *sekretess, riktighet, tillgänglighet och i vissa fall även spårbarhet* för högskolans informationsresurser.

Informationssäkerhetspolicy är högskolans övergripande dokument som anger mål och inriktning samt styr organisationens informationssäkerhetsarbete.

Ledningssystem för informationssäkerhet (LIS). Process för styrning och ledning av informations-säkerhetsarbetet vid Högskolan Dalarna, vilket bland annat omfattar utformning av styrande dokument, organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder.

MSB. Myndigheten för samhällsskydd och beredskap. MSB har bland annat i uppgift att samordna arbetet med samhällets informationssäkerhet.

MSBFS 2009:10. MSB:s föreskrift om statliga myndigheters informationssäkerhet.

Skyddsnivå för en informationsresurs ska utformas enligt gällande lagar och förordningar. I övrigt ska skyddsnivåer väljas utgående från fortlöpande och systematiska risk- och hotbildsanalyser samt konsekvenser av störningar.

Skyddsåtgärder ska väljas utgående från fortlöpande och systematiska risk- och hotbildsanalyser samt konsekvenser av störningar. Skyddsåtgärder ska, där det är möjligt, baseras på etablerade standarder eller de facto-standarder inom informationssäkerhetsområdet.

SS-ISO/IEC 27001. Svensk och internationell standard som tillhandahåller en modell för att upprätta, införa och driva, övervaka och granska, samt underhålla och förbättra ett ledningssystem för informationssäkerhet.

4 Mål

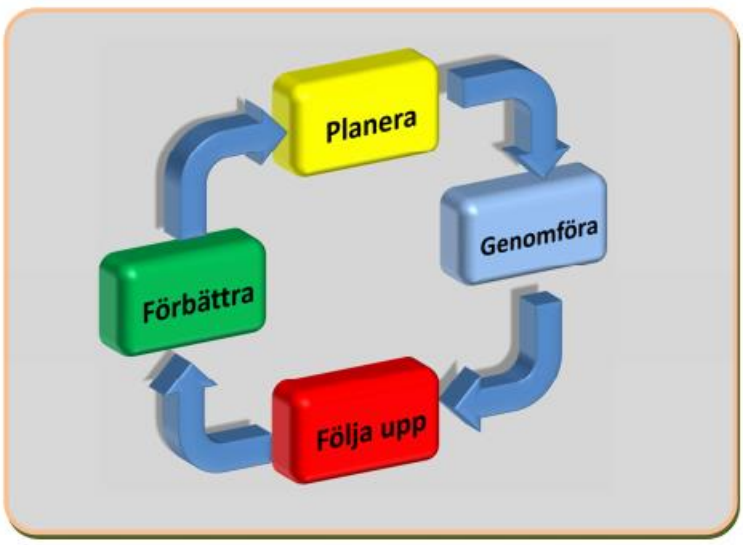
Det övergripande målet är att upprätthålla en väl avvägd informationssäkerhet med hänsyn till behoven hos högskolan, verksamma vid högskolan och allmänheten samt att värna om högskolans uttalade viljeinriktning att vara en öppen högskola. Det handlar om att balansera risker (sannolikhet och konsekvens) mot kostnader för skyddsåtgärder - uppnådd balans är detsamma som *Rätt säkerhet*.

5 Modell och metodik

Högskolan Dalarna har valt att arbeta enligt den så kallade PDCA-metoden (”plan, do, check, act”), vilken också är den av MSB rekommenderade modellen och metodiken vid implementation av LIS.

Metodstödet beskriver en process och när det gäller informationssäkerhet går PDCA-metoden ut på att ständigt förbättra arbetssätt och säkerhetslösningar i en iterativ process. På detta sätt erhålls ett strukturerat arbete som syftar till att analysera och mäta både nya och gamla företeelser, planera åtgärder som sedan införs, och som i sin tur granskas och leder till nya förbättringar.

Informationssäkerhetsarbetet ska styras och utföras enligt högskolans LIS och enligt nedanstående process för planering, genomförande, uppföljning och förbättring.



5.1 Omfattning

Detta avsnitt är strukturerat enligt de fyra processtegen planering, genomförande, uppföljning och förbättring. Det anger övergripande krav på skyddsåtgärder inom de säkerhetsområden som omfattas av LIS.

5.1.1 Planering

Implementeringen av LIS och därefter löpande förbättringsåtgärder planeras i samband med verksamhets- eller systemförvaltningsplanering och sker på högskoleövergripande nivå, för en akademi eller avdelning, för ett förvaltningsobjekt eller ett enskilt informationssystem. Uppföljning sker sedan på årlig basis.

Både implementationen av LIS samt tillkommande ändringskrav ska vara baserade på risk- och hotbildsanalyser och ange beslutade skyddsåtgärder för de säkerhetsområden som anges i 5.1.2. Genomförande. För detta finns mallar och anvisningar för risk- och hotbildsanalyser.

Löpande förbättringsåtgärder ska införas som ett resultat av periodiskt uppföljnings- och förbättringsarbete i punkterna 5.1.3. Uppföljning och 5.1.4. Ständiga förbättringar.

Därutöver kan säkerhetsförbättringar vid behov införas utom plan, t.ex. vid allvarliga incidenter, införande av nya informationssystem eller IT-tjänster, säkerhetsuppdateringar i programvaror, etc.

5.1.2 Genomförande

Det operativa säkerhetsarbetet som innebär att driva, mäta och följa upp så att LIS, enligt planering och beslut enligt punkt 5.1.1. ger avsedd säkerhetsnivå inom nedanstående områden, se underrubriker.

5.1.2.1 Policy för informationssäkerhet

Högskolan Dalarnas policy för informationssäkerhet anger övergripande mål och regler för högskolans informationssäkerhetsarbete.

5.1.2.2 Övriga styrdokument för informationssäkerhet

Plan för informationssäkerhet (detta dokument) samt olika regeldokument ska beslutas och implementeras under 2015.

Föreliggande regeldokument:

- Regler för användande av Högskolan Dalarnas IT-resurser
- Informationssäkerhetsregler för användare inom Högskolan Dalarna
- Regler för destruktion av elektronisk utrustning vid Högskolan Dalarna
- Uppdatering av systemägarförteckning inom Högskolan Dalarna

- Utöver de formella styrdokumenten finns också en IT-handbok som utgår ifrån SUSECs[1] handbok (länk till handboken: http://itsakhandbok.irt.kth.se/).
  - Den anpassade versionen för Högskolan Dalarna genomgår en omarbetning under 2015
  - Handboken går i detalj in på olika sidor av hanteringen av digital information, vad man bör tänka på, hur man bör arbeta och vilka risker som finns. Handboken är ett levande dokument och uppdateras regelbundet. Den är inte tänkt att sträckläsas utan skall istället utgöra en källa till kunskap kring specifika frågor inom informations- och IT-säkerhet

5.1.2.3 Hantering av informationstillgångar

Grundläggande krav för hantering av högskolans informationsresurser är att:

- de ska vara identifierade och dokumenterade
- skyddsåtgärder med avseende på sekretess, riktighet och tillgänglighet, samt i vissa fall även spårbarhet, är baserade på högskolans anvisningar för informationsklassificering

[1] Swedish University information SECurity group (SUSEC), är en oberoende, ideell förening av personer, anställda vid universitet och högskolor, och som huvudsakligen arbetar med informationssäkerhet. Föreningen skall verka i första hand inom Universitets- och Högskolevärlden för erfarenhetsutbyte och kompetensuppbyggnad inom området informations- och IT-säkerhet höjning av säkerheten i system, applikationer och nät, spridandet av kunskap om informationssäkerhet samt samverka med samhällets olika organ inom området.

5.1.2.4 Personalresurser och informationssäkerhet

Informationssäkerhetsansvarig ansvarar för att aktuell och lättillgänglig information om informationssäkerhet och relaterade styrdokument finns på högskolans intranät, Du & Ja.

Informations- och utbildningsinsatser ska erbjudas de verksamma. För ytterligare stöd finns möjlighet att kontakta informationssäkerhetsansvarig.

Verksamma inom Högskolan Dalarna erbjuds en intern webbaserad introduktionsutbildning, *Datorstödd informationssäkerhetsutbildning för användare (DISA[2])*, som på ett enkelt och kostnadseffektivt sätt höjer medarbetarnas medvetenhet om, och grunderna i, en god informationssäkerhetshantering.

5.1.2.5 Fysisk och miljörelaterad säkerhet

Lokaler och utrustning som är avsedda för högskolans informationshantering ska vara utrustade med ett väl avvägt skydd mot intrång, otillåten användning, stöld, brand och annan skada.

5.1.2.6 Styrning av åtkomst till information och informationstillgångar

Inom högskolan baseras åtkomsträtten till information på Tryckfrihetsförordningens offentlighetsprincip, offentlighets- och sekretesslagen samt personuppgiftslagen (PUL).

Alla informationssystem ska ha rutiner och system för behörighetskontroll för att förhindra otillåten åtkomst, förändring eller förstöring av information.

5.1.2.7 Anskaffning, utveckling, underhåll samt avveckling av informationssystem

För att säkerställa att säkerhet är en integrerad del av högskolans informationssystem ska

- en risk- och hotbildsanalys genomföras i alla utvecklings- och anskaffningsprojekt
  - Ansvarig: Projektägare/motsvarande
  - Status: Rutin ska implementeras under 2015
- planering och uppföljning av skyddsåtgärder görs som en del av det löpande förvaltningsarbetet med befintliga informationssystem
  - Ansvarig: Systemägare/motsvarande
  - Status: Pågående
- gallring och bevarande av handlingar sker i enlighet med Riksarkivets föreskrifter
  - Ansvarig: Informationsägare
  - Status: Pågående
- avveckling av informationssystem sker på ett kontrollerat sätt
  - Ansvarig: Systemägare/ motsvarande
  - Status: Rutin ska implementeras under 2015
- destruktion av elektronisk utrustning sker i enlighet med regeldokument
  - Ansvarig: IT-avdelningen samt säkerhetsansvarig
  - Status: Regel och rutin ska implementeras under 2015

I samband med upphandlingar av IT-relaterade tjänster och produkter ska alltid krav baserade på informationssäkerhetssynpunkt ingå som en obligatorisk del. En mall finns framtagen för detta ändamål som täcker områdena:

- *Fysisk säkerhet*
- *Åtkomst och behörigheter*
- *Spårbarhet och övervakning*
- *Nätverk*
- *Kryptering*
- *Leverantörens säkerhetsansvar*
- *Backup och kontinuitet*
- *Applikationer*
- *Motståndskraft vid angrepp*
- *Dokumentation*

[2] DISA är producerat av MSB och tillhandahålls fritt. Möjligheter finns att installera systemet i den lokala IT-miljön och då finns även möjlighet att göra lokalt anpassade svarsalternativ. Högskolan Dalarna har valt att göra vissa anpassningar.

5.1.2.8 Hantering av informationssäkerhetsincidenter

Löpande bevakning, uppföljning och rapportering av informationssäkerhetsincidenter, t.ex. om en dator utsatts för intrång eller intrångsförsök, ska göras av högskolans IT-avdelning.

Verksamma ska vid behov rapportera informationssäkerhetsincidenter. Inrapportering sker via telefon till IT-supporten eller mail till support@du.se.

5.1.2.9 Kontinuitetsplanering för informationssystem

Avbrottsplanering ska genomföras för alla informationssystem som stödjer verksamhet där längre avbrott kan orsaka stor skada för högskolan, verksamma vid högskolan och andra berörda. Avbrottsplanen ska ingå i högskolans systemförvaltningsmodell.

Baserad på prioriteringar i verksamheternas avbrottsplaner ska en återstartsplan finnas inom IT-organisationen för återgång till drift av ordinarie system.

Såväl avbrotts- som återstartsplaner ska testas regelbundet.

5.1.2.10 Efterlevnad

För att säkerställa efterlevnad av LIS i förvaltningsobjekt, informationssystem och utvecklingsprojekt samt att högskolan säkerhetsarbete följer tillämpliga lagar, föreskrifter och avtals-förpliktelser ska:

- verksamhetsgenomgång för identifikation av högskolans informationstillgångar, identifikation av krav (legala och interna) samt klassificering av informationstillgångarna genomföras
  - Ansvarig: Avdelningschef eller systemägare, med stöd av informationssäkerhetsansvarig
  - Status: Pågående
- risk- och hotbildsanalyser enligt anvisningarna för risk- och hotbildsanalyser genomföras på regelbunden basis.
  - Ansvarig: Systemägare/motsvarande
  - Status: Pågående
- omvärldsbevakning av tillämplig lagstiftning och föreskrifter om statliga myndigheters informationssäkerhetsarbete ske på löpande basis
  - Ansvarig: Informationssäkerhetsansvarig
  - Status: Infört

5.1.3 Uppföljning

I detta processteg görs periodisk uppföljning och rapportering av hur LIS fungerar i verksamheten med avseende på uppsatta mål, praktisk erfarenhet och efterlevnad.

Förslag på förbättringsåtgärder läggs till grund för prioriteringar och beslut i punkt 5.1.4. Ständiga förbättringar.

Status: Då implementering av LIS pågår kommer detta processteg att initieras i samband med att LIS övergår i en förvaltningsfas.

5.1.3.1 Uppföljning av informationssäkerhetsincidenter

Högskolans IT-avdelning samt informationssäkerhetsansvarig planerar att på regelbunden basis följa upp och rapportera följande statistik till förvaltningschef samt säkerhetsansvarig:

- inrapporterade incidenter enligt punkt 5.1.2.8. Hantering av informationssäkerhetsincidenter under den senaste perioden och förändringar jämfört med tidigare perioder
- sammanställning av förebyggande eller korrigerande åtgärder under denna och föregående perioder och utfall av dessa

5.1.3.2 Uppföljning av efterlevnad

Högskolans IT-säkerhetsorganisation samt informationssäkerhetsansvarig ska på regelbunden basis följa upp och rapportera följande resultat till säkerhetsansvarig samt förvaltningschef:

- genomförda risk/hotbilds- och säkerhetsanalyser
- genomförda revisioner avseende informationssäkerhet
- konsekvenser av genomförda och kommande förändringar i tillämpliga lagar, föreskrifter och avtalsförpliktelser

5.1.4 Ständiga förbättringar

Målet är att arbeta med ständiga förbättringar genom att implementera LIS med avseende på funktionalitet och kvalitet genom korrigerande och förebyggande åtgärder, samt för bättre efterlevnad genom information och utbildning.

Förbättringsåtgärder ska vara baserade på ledningsbeslut, revisioner eller annan relevant information enligt punkt 5.1.3.

Förslag och prioriteringar av förbättringar i LIS ska ingå som en del av informationssäkerhetsansvarigs löpande planering och uppföljning av informationssäkerhetsarbetet samt utgöra underlag för högskolans årliga verksamhetsplan och verksamhetsuppdrag.

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

5.2 Implementering

Implementering av denna plan och underliggande stöddokument ska ske genom att

- aktuell och lättillgänglig information om informationssäkerhet tillhandahålls på högskolans intranät, Du & Ja.
- olika informations- och utbildningsinsatser erbjuds de verksamma.
- högskolans informationssäkerhetsansvarig samt IT-säkerhetsorganisation finns tillgänglig för kontakt via telefon, e-post och webb samt även för riktade informations- och utbildningssatsningar inom verksamheten.
- implementationsprojektet för införande av LIS fortskrider med de olika aktiviteterna
    - Verksamhetsgenomgång med identifikation av informationstillgångar, identifikation av krav, klassificering av informationstillgångar, risk- och sårbarhetsanalys samt upprättande av åtgärdsplaner
    - Arbetet med relaterade regeldokument fortskrider
- särskild uppmärksamhet ägnas implementering av plan för informationssäkerhet och övriga styrdokument gällande informationssäkerhet i systemförvaltningsarbetet