Informationssäkerhetspolicy

Innehåll

1 Inledning

Denna policy utgör grunden i Ladokkonsortiets ledningssystem för informationssäkerhet (LIS) och beskriver konsortiets ramverk för informationssäkerhet. Policyn ska utgöra ett stöd för verksamheten i det dagliga arbetet. Arbetet med informationssäkerhet utgår främst från lagar, förordningar, föreskrifter, konsortiets 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 denna policy ska konsortiet:

- 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 konsortieledningens och den övriga organisationens ansvar för konsortiets 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 konsortiets 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 konsortiet ansvarar för.

2 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 konsortiets alla verksamhetsdelar. Detta då en säker informationshantering utgör en förutsättning för att vi skall kunna fullgöra uppdraget med att tillhandahålla säker utveckling och drift av Ladok.

3 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 (IT-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.

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

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

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.

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

4 Målsättning

Målet för informationssäkerhetsarbetet vid Ladokkonsortiet 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.

5 Roller och ansvar

Det övergripande ansvaret för konsortiet har styrelsen, vilket inbegriper ansvaret för informationssäkerhet. Styrelsen fastställer informationssäkerhetspolicyn och årlig verksamhetsplan.

Konsortiechef (KC) har det operativa ansvaret för informationssäkerhetsarbetet.

KC utser ansvarig för samordningen av informationssäkerheten. Informations-säkerhetsansvarig har ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerhetsarbetet.

KC utser Dataskyddssamordnare. Dataskyddssamordnaren fungerar som kontaktperson mot Datainspektionen och ansvarar för att hänsyn tas till Dataskyddförordningen inom konsortiet.

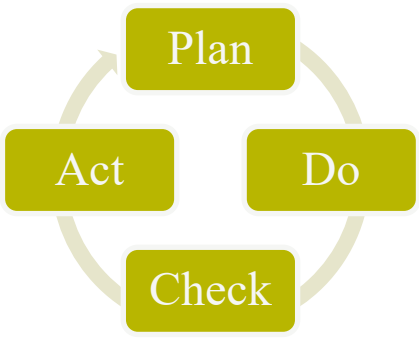
KC utser en grupp som har till uppgift att utgöra ett rådgivande beredande organ till stöd för informationssäkerhetsansvarig i informationssäkerhetsarbetet, bland annat genom att tillse att ledningssystemet för informationssäkerhet vid Ladokkonsortiet fungerar och efterlevs i dess olika delar. I detta organ ska följande funktioner finnas representerade:

KC, Produktägare, Dataskyddssamordnare, IT-Arkitekt samt övriga funktioner som KC beslutar ingå.

Enligt konsortieavtalet avtalet ansvarar lärosätet/partshögskolorna för en korrekt informationssäkerhetshantering utifrån aspekterna konfidentialitet, riktighet och tillgänglighet. Ladokkonsortiets ansvar som personuppgiftsbiträde regleras i bilaga 2 Personuppgiftsbiträdesavtal till konsortieavtalet.

6 Arbetssätt

Arbetssätt i Ledningssystemet för informationssäkerhet vid Ladokkonsortiet bygger på PDCA-modellen enligt de övergripande stegen Planera, Genomföra, Utvärdera och Förbättra. Varje steg innehåller i sin tur en eller flera processer.



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.

Genomföra – Driva och genomföra det faktiska informationssäkerhetsarbetet. Risk och sårbarhetsanalysen utgår från ovan nämnda kartläggning och klassificeras därefter utifrån MSBs modell för klassificering av information med en bedömning av respektive process säkerhetsaspekt (konfidentialitet, tillgänglighet samt riktighet) samt konsekvensnivå.

Utifrån risk- och sårbarhetsanalysen upprättas inför varje år en handlingsplan som KC fastställer. Handlingsplanen ska innehålla föreslagna åtgärder, status och ansvariga. De övergripande målen för handlingsplanen fastställes i konsortiets verksamhetsplan för året.

Konsortiets medarbetare utbildas/informeras om informationssäkerhetsansvaret utifrån befattning och ansvar. Medarbetarna informeras om sitt informationssäkerhetsansvar åtminstone en gång per år.

Kontinuitetsplaneringen består av en kontinuitetsplan som gäller för Konsortiets verksamhet. I denna beskrivs de rutiner som finns för att verksamheten inom Ladokkonsortiet ska kunna fungera vid en katastrof. Kontinuitetsplanen är avsedd att användas i situationer som definierats som en katastrof, men ska även vara ett stöd i avbrottsplaneringen.

Incidenthanteringen hanteras enligt fastställd process. 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 Ladokkonsortiet fungerar och efterlevs. Denna policy skall 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 konsortiets verksamhetsplan görs en genomgång av risk- och sårbarhetsanalysen och vilka åtgärder som vidtagits under föregående år. Nya övergripande mål tas fram för informationssäkerhetsarbetet samt en ny handlingsplan fastställs. Därutöver sker en kvartalsvis rapportering av informationssäkerhetsarbetet i samband med uppföljningen av verksamhetsplanen till styrelsen.

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

Genom att kartlägga och systematisera konsortiets 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. En generell information om LIS som vänder sig till alla inom konsortiet ska finnas tillgänglig på Konsortiets interna webb (Confluence) för att öka medvetenheten om risker och hot inom området.