



Informationssäkerhetspolicy

Innehåll

1. INLEDNING	3
2. DEFINITIONER	3
3. MÅL	4
4. STYRNING OCH ARBETSSÄTT	4
5. ROLLER OCH ANSVAR	5
6. INCIDENT- OCH KONTINUITETSHANTERING	5

1 Inledning

Ladokkonsortiet ansvarar för vidareutveckling, drift och support av det nationella utbildningsadministrativa system Ladok åt 40 lärosäten. Denna policy utgör grunden i Ladokkonsortiets ledningssystem för informationssäkerhet (LIS) och beskriver konsortiets ramverk för cybersäkerhet och informationssäkerhet. Policyn ska utgöra ett stöd för verksamheten i det dagliga arbetet. Arbetet med informationssäkerhet utgår från i huvudsak dessa lagar, förordningar, föreskrifter, konsortiets egna krav samt avtal:

- Förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor
- MSBFS 2020:6, 2020:7 och 2020:8
- Dataskyddsförordningen
- Offentlighets- och sekretesslagen
- Konsortialavtal
- Avtal om gemensamt personuppgiftsansvar
- Personuppgiftsbiträdesavtal Ladoksystemet

Konsortiets ledningssystem för informationssäkerhet är systematiskt och riskbaserat med stöd av standarden SS-EN ISO/IEC 27001:2022, 27002:2022 samt 27701:2021.

2 Definitioner

Cybersäkerhet är informationssäkerhet avseende indirekta och direkta, externa beroenden och hot som finns i ett större och mer komplext digitalt ekosystem än (enbart) inom den egna organisationen eller samhället.

Hot är möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten.

Informationstillgångar är information och informationsbehandlande resurser som är av värde för en organisation.

Informationssäkerhet är skydd av informationstillgångar avseende konfidentialitet, riktighet och tillgänglighet. Informationssäkerhet kan uppnås genom en uppsättning säkerhetsåtgärder för bevarande av informationens egenskaper. Informationssäkerhet omfattar områdena organisatorisk säkerhet och teknisk säkerhet.

Konfidentialitet är egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Ladok är ett nationellt, studieadministrativt system som vidareutvecklas, drifas och supportas av Ladokkonsortiet.

Ladokkonsortiet är samarbetsorganisationen som ansvarar för systemet Ladok samt ett antal kringtjänster.

Mål är resultat som ska uppnås.

Riktighet är egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.

Risk är osäkerhetens effekt på mål.

Systematiskt och riskbaserat informationssäkerhetsarbete innebär att organisationen löpande identifiera kritiska informationstillgångar och inför säkerhetsåtgärder för att skydda den.

Team, Ladokkonsortiets verksamhet är organiserad i ett antal team.

Tillgänglighet är egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning.

3 Mål

Målet för informationssäkerhetsarbetet vid Ladokkonsortiet är att skydda dess informationstillgångar mot olika hot och att skapa en effektiv hantering och rutiner för att säkerställa att system och information omfattas av säkerhetsaspekterna konfidentialitet, tillgänglighet samt riktighet. Säkerhet ska ingå i det löpande utvecklingsarbetet.

Informationssäkerhetsarbetet är en del av vårt löpande arbete och alla medarbetare är säkerhetsmedvetna samt har god kunskap om hur de i sitt dagliga arbete kan förbättra informationssäkerheten inom Ladokkonsortiet.

4 Styrning och arbetssätt

Information är en av konsortiets viktigaste tillgångar och utgör en förutsättning för att bedriva verksamheten. Informationstillgångarna 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 kunna fullgöra uppdraget med att tillhandahålla säker utveckling och drift av Ladok.

I arbetet mot Ladokkonsortiets vision finns mål och strategier i en strategikarta som uppdateras och prioriteras löpande, där hanteras även informationssäkerhet. Ladokkonsortiets löpande arbete planeras kvartalsvis i en produktbacklog. Informationssäkerhetsarbetet bedrivs riskbaserat där gap identifieras och åtgärder prioriteras och arbetas med löpande. De risker som identifieras sammanställs och avrapporteras till styrelsen årligen.

Konsortiet arbetar systematiskt och riskbaserat och identifierar löpande kritiska informationstillgångar som är viktiga och inför löpande säkerhetsåtgärder för att skydda dessa.

Kontinuerlig omvärldsbevakning och förändringar till interna arbetssätt leder till behov av förändringar till ledningssystemet för informationssäkerhet identifieras. Ledningssystemet för informationssäkerhet med tillhörande regler och riktlinjer revideras löpande.

Ladokkonsortiets leverantörer omfattas av konsortiets arbetssätt och krav angående informationssäkerhet, detta regleras i respektive avtal.

5 Roller och ansvar

Det övergripande ansvaret för cybersäkerhet och informationssäkerhet inom Ladokkonsortiet har styrelsen. Konsortiechefen har det operativa ansvaret för informationssäkerhetsarbetet och utser en Dataskyddsamordnare samt en Informationssäkerhetsansvarig. Ansvaret för informationssäkerheten i Ladokkonsortiet delegeras inom organisationen via följande roller:

- Dataskyddssamordnaren fungerar som kontaktperson mot Datainspektionen och lärosätena, samt ansvarar för att Dataskyddförordningen följs inom konsortiet.
- Informationssäkerhetsansvarig har ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerhetsarbetet.
- Strategisk produktägare ansvarar för att produkten uppfyller kraven på säkerhet.
- Arkitekten ansvarar för att arkitekturen uppfyller kraven på säkerhet.
- Driftansvarig ansvarar för att driftmiljöerna uppfyller kraven på säkerhet.

Teamen har ansvar för att identifiera och hantera informationssäkerhetsrisker i utveckling av sina delar av systemet.

Konsortiechefen utser även en grupp som har till uppgift att utgöra ett rådgivande beredande organ till stöd för informationssäkerhetsansvarig.

Enligt konsortieavtalet äger och ansvarar lärosätena för sin information i Ladok. Lärosätena har reglerat sitt gemensamma personuppgiftsansvar i Avtal om gemensamt personuppgiftsansvar, bilaga 1, där även en särskild reglering av lärosätenas inbördes ansvar för personuppgiftsbehandling finns. Varje lärosäte ansvarar för att ha ett systematiskt och riskbaserat informationssäkerhetsarbete.

6 Incident- och kontinuitetshantering

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 kris. Kontinuitetsplanen är avsedd att användas i situationer som definierats som en kris, 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.