Handlingsplan för informationssäkerhet 2026

Försvarshögskolan

Försvarshögskolans informationssäkerhetplan 2026

Styrdokument:	Försvarshögskolans informationssäkerhetplan 2026
Klassificering	Plan
Diarienummer	Ö 296/2025
Beslutsfattare	Rektor
Dokumentansvarig	C IT
Senaste beslutsdatum	2026-03-20
Giltighetstid	Informationssäkerhetsplanen ses över och uppdateras årligen i FHS planeringsprocess
Dokument som ersätts	FHS informationssäkerhetsplan 2025
Relaterade dokument	Försvarshögskolans verksamhetsplan 2026, där informationssäkerhetplanen utgör ett appendix
Kortare sammanfattning	I FHS handlingsplan beskrivs de målsättningar inom informationssäkerhetsområdet som högskolans myndighetschef fastställt. Målen ger en inriktning för den utveckling som ska genomföras i syfte att vidmakthålla en fullgod informationssäkerhet.

Innehåll

1 Inledning

Försvarshögskolan (FHS) ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS). Informationssäkerhet är en viktig verksamhetsfråga, det konkretiserar verksamhetens behov av olika skyddsåtgärder vilket leder till bättre kontroll och skydd av FHS informationstillgångar. Digitalisering och utvecklingen av informationshantering i kombination med en ökad och förändrad omvärldsbild innebär att informationssäkerhet är en förutsättning och nödvändighet för att verksamheten ska kunna bedrivas i det digitala samhället.

Enligt myndigheten för samhällsskydd och beredskap (MSB) föreskrifter (MSBFS 2020:6) ska alla statliga myndigheter bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS) och beakta standard ISO/IEC 27001.

2 Organisation och ansvar

Ledningens engagemang och en tydlig ansvarsfördelning är avgörande för ett framgångsrikt informationssäkerhetsarbete. På Försvarshögskolan är det rektor som har det yttersta ansvaret för ledningssystemet för informationssäkerhet (LIS). Vid ledningens genomgång, som genomförs i samband med ordinarie T1-uppföljning redovisas det gångna årets informationssäkerhetsarbete och ledningen fattar beslut om inriktning för det fortsatta arbetet.

Respektive organisationsenhetschef (C OrgE) ansvarar för att policys, handlingsplaner, utbildning och regler tillämpas och integreras i verksamheten. I handlingsplanens aktivitetslista finns också utpekat vilken funktion som ansvarar för respektive aktivitet. Informationssäkerhetssamordnaren har ett samordningsansvar för uppföljning och uppdatering av handlingsplanen samt för högskolans ledningssystem för informationssäkerhet i sin helhet. Ansvaret för enskilda medarbetare omfattar att följa policys, handlingsplaner, regler, delta i utbildningar och rapportera incidenter.

3 LIS (Ledningssystem för informationssäkerhet)

Försvarshögskolans ledningssystem för informationssäkerhet (LIS) bygger på kraven i MSBFS 2020:6 och standarderna SS-EN ISO/IEC 27001/27002/27702, och omfattar även behandling av personuppgifter.

LIS inkluderar informationssäkerhetspolicy, informationssäkerhetsmål, handlingsplan, roller och ansvarsfördelning, dokumenterade regler och rutiner, intern informationssäkerhetsrevision, riskanalys och årlig uppföljning. För att nå målen ska det finnas en handlingsplan med aktiviteter samt tidsplan och ansvar för genomförande. Myndigheten ska även arbeta med information och utbildning för personalen samt säkerställa att informationssäkerhetskrav integreras i samtliga upphandlingar och avtal. Uppföljning av LIS och årlig utvärdering av informationssäkerhetsarbetet sker genom ordinarie styrprocesser.

Ett väl fungerande LIS är viktigt för att skydda informationstillgångar då det gör det möjligt att:

- Säkerställa att informationstillgångarna har ett fortlöpande fullgott skydd mot hot.
- Upprätthålla en strukturerad och övergripande process för att identifiera, bedöma och reducera informationssäkerhetsrisker,
- Applicera relevanta säkerhetsåtgärder samt kontinuerligt mäta och förbättra dess effektivitet.
- Ständigt förbättra säkerhetsnivån och på ett effektivt sätt säkerställa efterlevnad av legala krav.

4 Mål

Målen syftar till att stärka FHS informationssäkerhet vilket samtidigt leder till att några av FHS strategiska risker reduceras samt bidrar till att uppfylla FHS övergripande mål.

Handlingsplanen bygger på T1 rapporteringen för ledningssystemet för informationssäkerhet och består av uppgifter som ska bidra till måluppfyllnad och är framtagna utifrån:

- Verksamhetens riskanalyser.
- Genomförd revision.
- Säkerhetshöjande åtgärder kopplat till LIS.
- GAP-analys mot MSB föreskrifter om informationssäkerhet och IT-säkerhet.

5 Aktiviteter 2026

Under 2026 fokuserar arbetet på att stärka informations- och cybersäkerheten genom att vidareutveckla informationsklassning, och förbättra interna arbetssätt. Arbetet omfattar både tekniska och organisatoriska åtgärder, såsom nya och förbättrade stödverktyg, stärkt incidenthantering, kontinuitetsplanering och riktade utbildningsinsatser. Ett annat prioriterat område är att utveckla arkitekturen för processer, information och system för ökad helhetsstyrning. Verksamhetsstödet kommer även att analysera den nya cybersäkerhetslagen (NIS2) och genomföra nödvändiga åtgärder.

5.1 Tekniska skyddsåtgärder (IT-säkerhet)

- Nytt ITSM-verktyg[1] för hela FHS för att förbättra struktur, spårbarhet och kontroll över ärenden, incidenter, förändringar och IT-tillgångar och bättre uppföljning.
- Automatisera informationsklassning.
- Genomföra aktiviteter för att säkerställa ett systematiskt IT- och cybersäkerhetsarbete.
- Införa IT och verksamhetsarkitektur som ger en helhetsbild av verksamhetens processer, information och IT-system. Förbättrar bland annat arbetet med att identifiera risker, ställa rätt säkerhetskrav och bygga in skydd i både verksamhet och tekniska lösningar.

[1] Ett ITSM-verktyg (IT Service Management-verktyg) är ett system som används för att planera, leverera, hantera och följa upp IT-tjänster i en organisation

- Ta fram stöd för att lagra och tillgängliggöra forskningsdata.
- Genomföra åtgärder för att stärka säkerheten i användningen av mobila enheter

5.2 Organisatoriska och administrativa skyddsåtgärder

- Fortsätta arbetet med att hitta effektiva former och processer kring informationsklassning inom forskning, utbildning och stödverksamhet.
- Se över hur utbildning och information kan inkorporeras i verksamheten för att säkerställa god säkerhetskultur.
- Genomföra åtgärder från cybersäkerhetskollen för att fortsätta förbättringsarbetet på informations- och cybersäkerhetsområdet.
- Se över incidentprocessen.
- Fortsätta arbetet med kontinuitetshantering.
- Fortsätta arbetet med att säkerställa korrekt informationshantering relaterat till NATO.
- Analysera den nya cybersäkerhetslagen (NIS2) och genomföra nödvändiga åtgärder

5.3 Dataskydd (GDPR)

- Se över de verktyg som finns för behandlingsregister, utbildning och DPIA att de är ändamålsenliga.
- Tydliggöra organisation och ansvar kring dataskyddsfrågor.

5.4 Ledningssystemet (LIS)

- Se över mål och indikatorer i LIS för tydligare uppföljning av informationssäkerhetsarbetet.
- Tydliggöra hur aktiviteter i handlingsplanen och åtgärder från riskanalyser relaterar till informationssäkerhetsmålen.
- Genomföra åtgärder från cybersäkerhetskollen för att fortsätta förbättringsarbetet på informations- och cybersäkerhetsområdet.

6 Uppföljning

Handlingsplanen uppdateras varje år utifrån ordinarie styrprocesser. Detta innebär att i T2-uppföljningen görs en bedömning av hur arbetet med aktiviteterna fortlöper medan det i T3 sker en slutlig uppföljning av aktiviteterna. Vid uppföljningen kan planen korrigeras och avvikelser kan upptäckas från lagd plan. Planen kan också utgöra ett underlag för den planering som görs för nästkommande år. Vid ledningens genomgång, som genomförs i samband med ordinarie T1-uppföljning redovisas det gångna årets informationssäkerhetsarbete och ledningen fattar beslut om inriktning för det fortsatta arbetet.

Försvarshögskolan