Informationssäkerhetsplan 2023

Försvarshögskolan

Försvarshögskolans handlingsplan för informationssäkerhet 2023

Styrdokument:	Försvarshögskolans handlingsplan för informationssäkerhet 2023
Klassificering	Plan
Diarienummer	Ö 76/2022
Beslutsfattare	Rektor
Dokumentansvarig	C IT
Senaste beslutsdatum	2023-02-24
Giltighetstid	2023, informationssäkerhetsplanen ses över och uppdateras årligen i FHS planeringsprocess
Dokument som ersätts	4/2021, FHS informationssäkerhetsplan 2022
Relaterade dokument	Informationssäkerhetsplanen utgör en bilaga till FHS övergripande verksamhetsplan
Kortare sammanfattning	I FHS handlingsplanen framkommer de målsättningar inom informations-säkerhetsområdet som FHS ledning fastställt. Målen ger en inriktning för den utveckling som FHS ska genomföra i syfte att vidmakthålla en fullgod informationssäkerhet.

Innehåll

Försvarshögskolan

1 Bakgrund

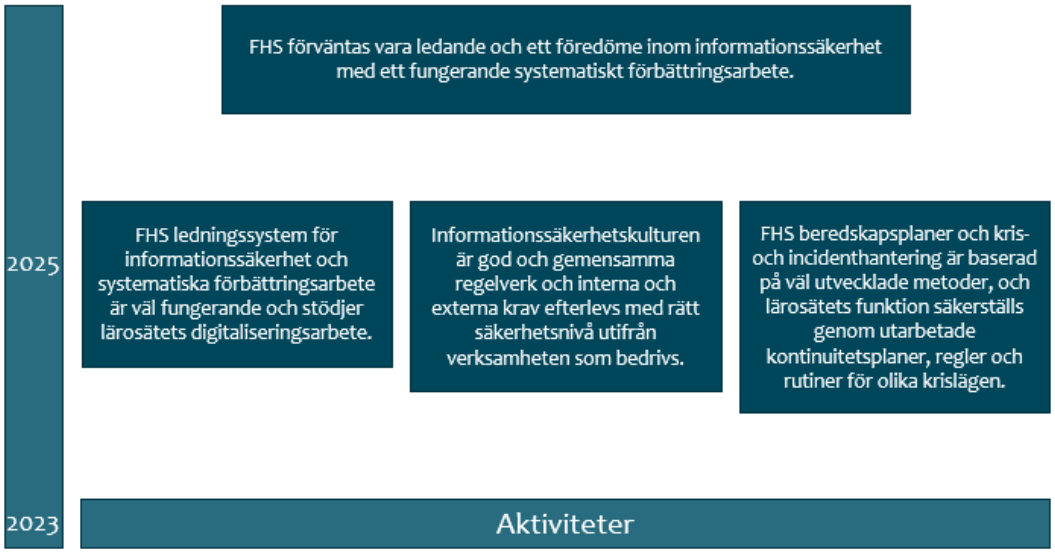
Försvarshögskolan (FHS) ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS). Informationssäkerhet är en viktig verksamhetsfråga och arbetet med informationssäkerhet ger stor verksamhetsnytta när det gäller att kartlägga vilka hot och risker som verksamheten ställs inför. 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 hotbild 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 Mål

Högskoleledningens förhållningsätt och principiella ställningstagande avseende informationssäkerhet finns fastställt i FHS informationssäkerhetspolicy. I FHS handlingsplan för informationssäkerhet fastställer högskoleledningen inriktningen för utvecklingen av informationssäkerhetsarbetet.

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.



BOX 278 05, 115 93 STOCKHOLM
BESÖKSADRESS: DROTTNING KRISTINAS VÄG 37 TEL: 08-553 425 00

Handlingsplanen bygger på T1 rapporteringen för ledningssystemet för informationssäkerhet och består av aktiviteter 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.

3 Planerade granskningsinsatser

3.1 Internrevision

Inriktning för revisionen 2023 är uppföljning av 2021 år revision på ledningssystemet för informationssäkerhet (LIS). Det innebär att kontrollera:

- Om informationssäkerhetsarbetet stöds av ett ändamålsenligt utformat ledningssystem för informationssäkerhet (LIS), i enlighet med MBS:s föreskrift 2020:6 kompletterat med utvalda krav från ISO/IEC 27001.
- I vilken utsträckning rutiner och dokumentation för att efterleva kraven i EU:s dataskyddsförordning (GDPR) med tillhörande genomförandeförfattningar, enligt ISO/IEC 27701, är implementerat i verksamheten.

Revision genomförs av Nixu AB.

3.2 Riksrevisionen

Riksrevisionen granskar Försvarshögskolan avseende informationssäkerhet och skydd av forskningsdata.

4 Utvecklingsområden

2023 kommer informationssäkerhetsarbetet fokusera på kontinuitetsarbete, införandet av informationsklassning och tydliggöra ansvar, hantering och förutsättningar och förväntningar ute i organisationen kring informationssäkerhet och dataskydd (GDPR).

Flera aktiviteter har påbörjats inom dessa områden och även funnits med som aktiviteter i tidigare handlingsplaner för informationssäkerhet. Nu behöver det viktiga arbetet att förankra och tillämpa besluten påbörjas, både inom stöd och kärnverksamhet för att komma vidare med det systematiska informationssäkerhetsarbetet.

4.1 Aktiviteter

Kontinuitetsarbete

- Se över FHS kontinuitetsplanering (identifiera och åtgärda).
- Interagera kontinuitetsplaneringen med beredskapsplaneringen.
- Utveckla IT:s kontinuitetsplan för infrastruktur.
- Upprätta en rutin och genomföra test av IT:s kontinuitetsplan för infrastruktur.

IT-säkerhet

- Analysera, ta fram handlingsplan och genomföra åtgärder utifrån resultatet av mätningen av FHS cybersäkerhet.

Organisatoriska åtgärder

- Dokumentera och etablera processer och rutiner som saknas inom drift och förvaltning enligt revision 2022.

Dataskydd (GDPR)

- Se över och ta fram/revidera styr och stöddokument utifrån dataskyddsförordningen krav.

- Undersöka möjligheten och behovet för ”säkra meddelanden”
    - *En funktion för att kunna skicka och svara på meddelanden med känslig information på ett säkert och lagenligt sätt.*

- Säkerställa kraven och sätta rutiner för inbyggt dataskydd (Privacy by design)
    - *Inbyggt dataskydd (privacy by design är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas genom att se till att inte mer information än nödvändigt samlas in, delas ut eller visas när man utformar IT-system och rutiner.*

Ledningssystemet (LIS)

- Undersöka om det är möjligt att hitta indikatorer utifrån gapanalys och FHS interna mätning kring cybersäkerhet för att förbättra uppföljningen och utvärdering i LIS.

- Undersöka om det är möjligt att hitta indikatorer från MSB:s uppföljningsverktyg infosäkkollen och mognadsdialogen för att förbättra uppföljningen och utvärdering i LIS.

- Konkretisera hur rapportering kan ske kring LIS och dataskydd (GDPR) utöver ledningens genomgång vid T1.

- Revidera FHS Regler för rapportering av informationssäkerhetsincidenter avvikelser och förbättringsförslag o Ansvaret kring hanteringen av incidenterna behöver tydliggöras.

- Analysera nya versionen av ISO/IEC 27002:2022 och ny Bilaga A i ISO/IEC 27001 och hur det kan påverka informationssäkerhetsarbetet och FHS ledningssystem för informationssäkerhet.

5 Uppföljning

Handlingsplanen uppdateras varje år genom FHS ordinarie planeringsprocess. Detta innebär att planen följs upp i samband med FHS ordinarie T2 och T3-uppföljning. Aktiviteterna återfinns och redovisas i FHSVP23. 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.

Försvarshögskolan