Informationssäkerhetsplan 2021

Försvarshögskolan

Försvarshögskolan

Försvarshögskolans handlingsplan för informationssäkerhet 2021

Styrdokument	
Rubrik	FHS handlingsplan för informationssäkerhet 2021
Klassificering	Plan
Ärendenummer	5/2020
Beslutsfattare	Rektor
Dokumentansvarig	C IT
Beslutsdatum	2020-12-18
Giltighetstid	2021, handlingsplanen ses över och uppdateras årligen i FHS planeringsprocess.
Dokument som ersätts	3/2019
Antal bilagor	Handlingsplanen utgör en bilaga till FHS övergripande verksamhetsplan.
Kortare sammanfattning	I handlingsplanen framkommer de målsättningar inom informations-säkerhetsområdet som FHS rektor fastställt. Målen ger en inriktning för den utveckling som FHS ska genomföra i syfte att vidmakthålla en fullgod informationssäkerhet. Handlingsplanen är en del i FHS ledningssystem för informationssäkerhet.

Försvarshögskolan

Bakgrund

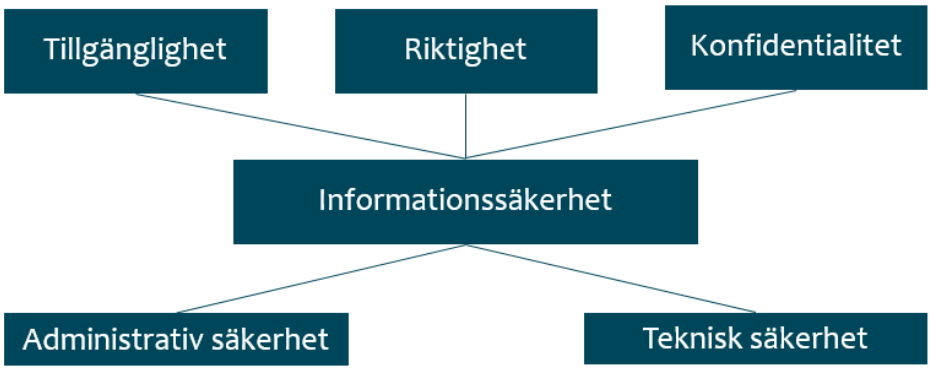
FHS ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS). Informationssäkerhet är en viktig verksamhetsfråga och arbetet med informationssäkerhet ger stor verksamhetsnytta när det gäller att kartlägga vilka hot och risker som verksamheten ställs inför. Det konkretiserar verksamhetens behov av olika skyddsåtgärder vilket leder till bättre kontroll och skydd av FHS informationstillgångar. Enligt myndigheten för samhällsskydd och beredskap (MSB) föreskrifter (MSBFS 2016:1) ska alla statliga myndigheter bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS) och beakta standard ISO/IEC 27001.

Information är en tillgång som behöver skyddas

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 effektivt i det digitala samhället.

Information är en tillgång som är avgörande för FHS verksamhet som behöver skyddas på ett lämpligt sätt genom att införa passande skyddsåtgärder. Informationssäkerhet omfattar skydd av all information oavsett form och innebär en strävan att skydda information så att:

- endast behöriga personer får ta del av informationen (**konfidentialitet**).
- informationen går att lita på, att den är korrekt och inte manipulerad (**riktighet**).
- informationen finns tillgänglig när den behövs (**tillgänglighet**).



Informationssäkerhetens skyddsåtgärder delas upp i två delar.

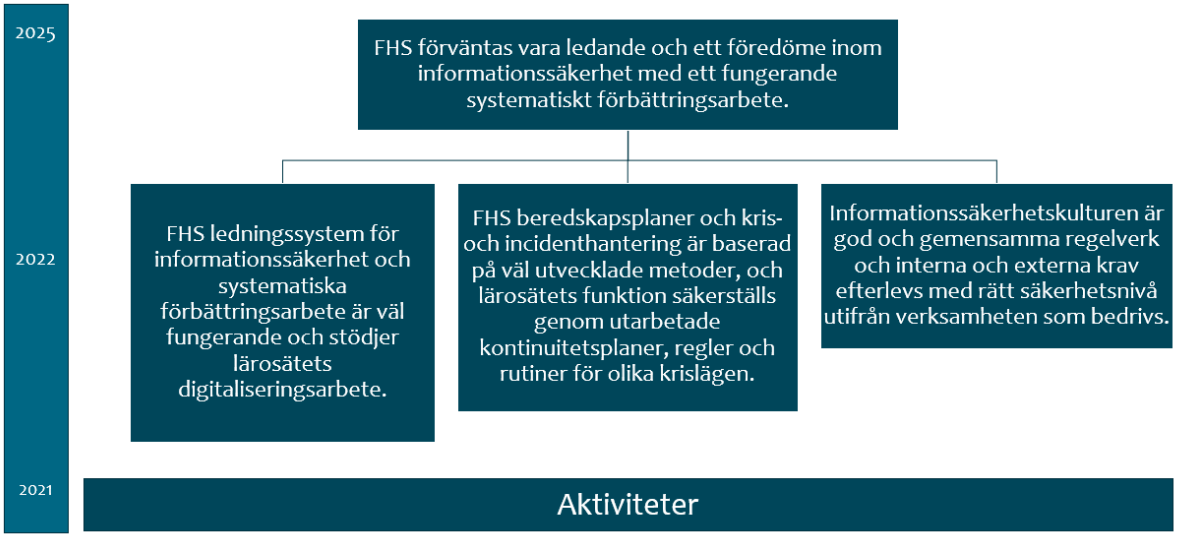
- Teknisk säkerhet som innefattar IT-säkerhet och fysisk säkerhet för att säkerställa exempelvis drift och tillgänglighet, larm och inpassering.
- Administrativ säkerhet som innefattar externa krav (lagkrav) och interna krav som policy, regelverk, rutiner, revison och uppföljning som FHS har för att säkerställa att verksamhetens information hanteras rätt. Det innefattar även utbildning och kommunikation för att skapa en informationssäker kultur där alla är medvetna om riskerna.

Försvarshögskolan

Mål och aktiviteter

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 strategiska mål.



Handlingsplanen består av aktiviteter som ska bidra till måluppfyllnad och är framtagna utifrån:

- Verksamhetens egna riskbedömningar och förslag till åtgärder.
- Genomförd revision.
- Säkerhetshöjande åtgärder kopplat till LIS.
- Säkerställa efterlevnad av MSB föreskrifter om informationssäkerhet och IT-säkerhet.

Aktiviteterna finns angivna i organisatoriska handlingsplaner där även ansvar och tidsramar framkommer.

Försvarshögskolan

Fokus 2021

Under 2021 kommer informationssäkerhetsarbetet fokusera mot följande områden och aktiviteter:

Skapa förutsättning för att förbättra spårbarhet, riktighet och konfidentialitet kring FHS information, dokumenthantering, identifiering och signering digitalt.

- Genomföra en förstudie kring dokumenthantering ur ett livscykelperspektiv (skapa, hantera, signera, lagra, dela, samarbeta, gallra, publicera) och avveckla/minimera P:.
- Införa digitala signaturer för interna beslut (W3D3).

Säkerställa att gällande lagkrav och föreskrifter efterlevs.

- Kartlägga kontinuitetshantering och planering och genomföra GAP-analys.

Förenkla incident- och avvikelserapporteringen för att bidra till det systematiska förbättringsarbetet

- Konsolidera avvikelsehantering oavsett typ (IT, säkerhet, fastighet m.m.)

FHS medarbetare har kännedom om regler, lagkrav och rutiner för att kunna bidra till en god säkerhetskultur.

- Utbildningsinsatser offentlig förvaltning och sekretess
- Se över möjligheterna till samordnad utbildning inom flera säkerhetsområden.

Systematisk förbättring av ledningssystemet för informationssäkerhet (LIS).

- Kartlägga skyddsåtgärder utifrån MBS´s föreskrifter och ISO 27001 och 27701.
- Fortsätta konsolideringen av GDPR och LIS.

Ledning och styrning av IT som strategisk resurs.

- Se över FHS Förvaltningsmodell och inarbeta IT-styrning i övergripande ledning och styrning.

Konsolidera antalet tjänster för att minska kostnader, öka säkerheten och skydda FHS information.

- Inventera molntjänster, cloud act/Schrem II/GDPR och säkra upp successivt.

Uppföljning

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