Informations- och IT-säkerhetsgruppen

Färdplansmässa 16 sep 2025

Stockholms universitet

Agenda 

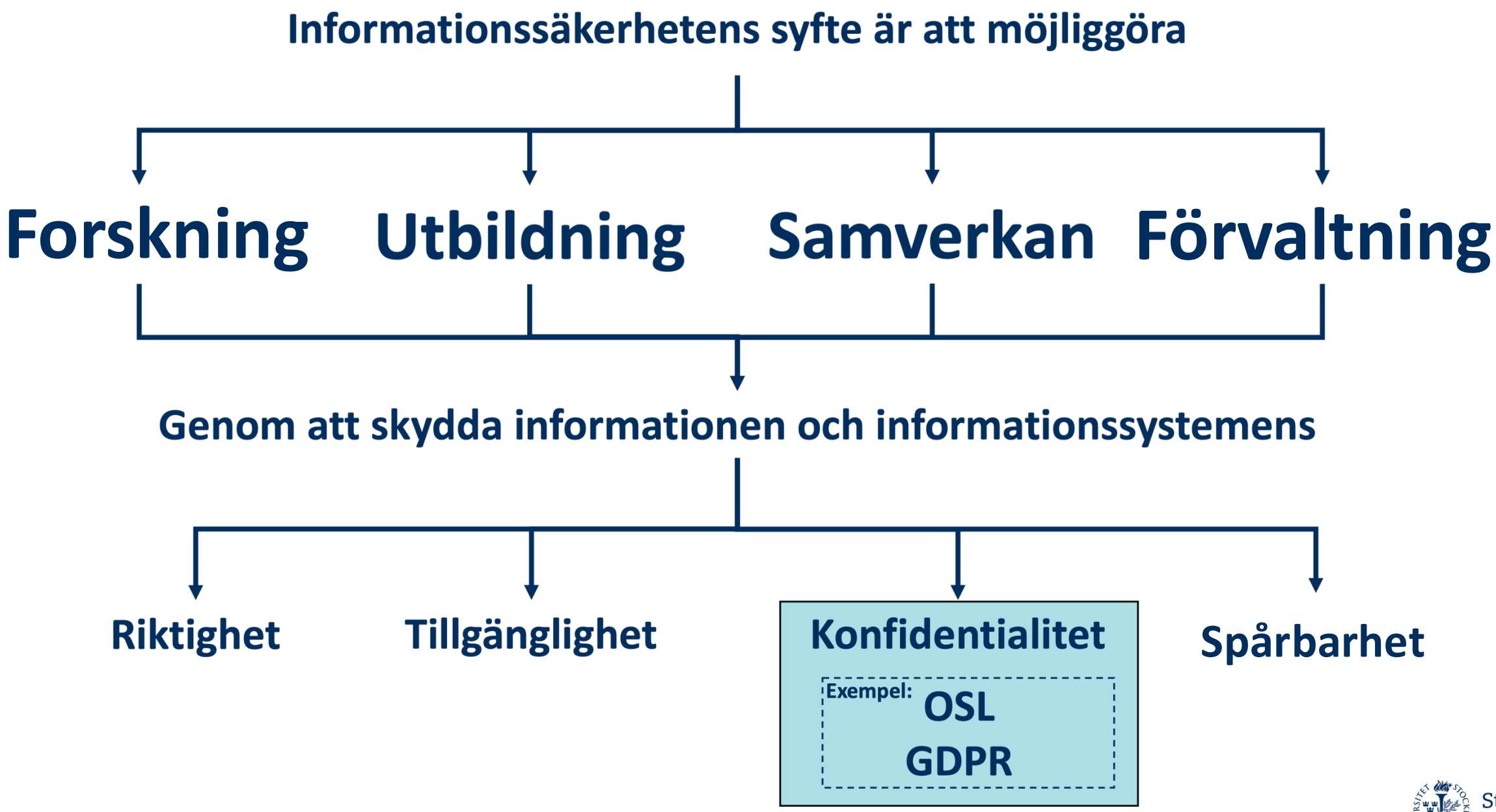
- Vårt uppdrag
- Hur vi jobbar
- Våra produktområden
- Åtgärdsplan

Stockholms universitet

Vårt uppdrag

Att skydda universitetets information och informationssystem för att skapa en säker grund för fri och effektiv akademisk verksamhet

Stockholms universitet



Stockholms universitet

Hur vi jobbar

- Agilt arbetssätt
- CISO – produktansvarig
- Teamcoach
- Produktsamordnare för varje område

Stockholms universitet

Produktområden

- IITS arbetar genom 8 olika produktområden
- Produktområden är framtagna för att fokusera arbetet inom IITS och för att ha ett gemensamt arbetsätt med resten av IT-avdelningen som är anpassat efter verksamhetens behov

Ledningssystem för informationssäkerhet (LIS)

Utbildning

Samverkan

Informationsklassificering

Upphandlingsstöd

Säkerhetskonfiguration

Säkerhetsövervakning

Incidenthantering

IITS produktområden

- **Informationsklassning** – För att veta vilket skydd som behövs måste vi först veta vilken information som faktiskt hanteras. Därför gör vi inventeringar av informationen, och utifrån det kan vi avgöra hur känslig den är och vilket skydd som krävs med hjälp av en klassning.

- **Utbildning** – vi arbetar kontinuerligt med att öka medvetenheten kring informationssäkerhet och IT-användning, bland annat genom riktade utbildningar i Nimblr och workshops inom M365.

- **Samverkan** – vi samordnar samarbeten internt och externt för att stärka universitetets säkerhet.

- **Upphandlingsstöd** – Vi arbetar tillsammans med upphandlingsenheten för att tidigt i processen definiera och ställa relevanta säkerhetskrav på nya IT-system. Genom att inkludera informationssäkerhet redan i kravställningen säkerställs att systemen stödjer universitetets behov av skydd för information och regelefterlevnad.

IITS produktområden

- **Ledningssystem för informationssäkerhet (LIS)** – Vi driver arbetet med universitetets ledningssystem för informationssäkerhet och tar fram stödmaterial som rutiner, riktlinjer och säkerhetspolicys. Vi stöttar även verksamheten genom att identifiera, bedöma och hantera risker.

- **Säkerhetskonfigurering** – här samarbetar vi nära med IT-grupperna för att systemen ska vara rätt inställda och säkra.

- **Säkerhetsövervakning** – vi följer upp och håller koll på hot och avvikelser i våra system.

- **Incidenthantering** – och när något faktiskt händer, då stöttar vi verksamheten från mindre phishingförsök till större incidenter

Sammanfattning

Vi har:

- ett tydligt uppdrag
- ett gemensamt arbetssätt
- åtta produktområden

Det är grunden för vår åtgärdsplan framåt

Åtgärdsplan för informations- och IT-säkerhet

Stockholms universitet

Bakgrund och omfattning

- Rektor har gett i uppdrag till IT-avdelningen att ta fram en plan i syfte att långsiktigt höja nivån på IT-säkerhetsarbetet och säkerställa en god IT-säkerhetsmiljö, vilket inkluderar att stärka det operativa IT-säkerhetsarbetet
- Vissa administrativa säkerhetsåtgärder har en sådan omfattning att de påverkar hela universitetet och därför kräver beslut av Rektor eller Universitetsdirektör. Till exempel vid översyn av besluts- och delegationsordningen eller vid införande av en ny handläggningsordning
- Den första fasen av arbetet med säkerhetsåtgärder kopplade till informationssystem kommer omfatta system och miljöer som hanteras och drivs av IT-avdelningen samt IT-avdelningens nätverk
- Påföljande arbete kommer även behöva innefatta miljöer som inte hanteras av IT-avdelningen som lokal IT och forsknings IT
- Internrevisionen har genomfört ett antal granskningar inom informations- och IT-säkerhet och Rektor har beslutat om åtgärder. Beslutade åtgärden som är inom IT-avdelningens ansvarsområde och som CISO har mandat över kommer att åtgärdas inom denna åtgärdsplan
- Ett ramverk har valts för att hjälpa att prioritera insatser baserad på verksamhetens behov, hotbild, och riskanalys.

Skyddsåtgärder

- Administrativa skyddsåtgärder
  - Översyn av besluts- och delegationsordningen inklusive CISO:s mandat att agera under aktiva incidenter
  - Inventering och klassificering av IT-system och tjänster så att tillgångar identifieras och klassificeras i enlighet med deras relativa betydelse för universitetets mål och riskstrategi (skyddsnivåer)
  - Uppdatera och upprätta styrdokument, processer, rutiner och andra stödmaterial - **(LIS arbete)**
- Tekniska skyddsåtgärder
  - Operativ säkerhetsövervakning av kritiska system och nätverk för att upptäcka avvikelser, indikatorer på intrång och andra potentiellt skadliga händelser. Inkluderar att bygga en avgränsad IT-miljö som är specialanpassad för att möta särskilda säkerhetskrav - **(under framtagning)**
  - Utveckling och implementering av lämpliga säkerhetskonfigurationer för system och tjänster
  - Tester av förmågan att snabbt återställa system och data vid incidenter
- Övriga skyddsåtgärder
  - Erbjuda utbildningar inom informations- och IT-säkerhet - **(mestadels genomfört)**
  - Samverkan mellan andra lärosätten, prefekter, avdelningar, CISO, informations- och IT-säkerhetsspecialister, IT-tekniker och DSA:er
  - Stöd vid upphandling av nya IT-system och tjänster via en informations- och IT-säkerhetskravkatalog - **(pågående)**
- Åtgärdsplanen täcker 3 år fram till 2028 för att nå en god nivå av informations- och IT-säkerhet. Därefter fortsätter arbetet systematiskt för att bibehålla nivån

Stockholms universitet