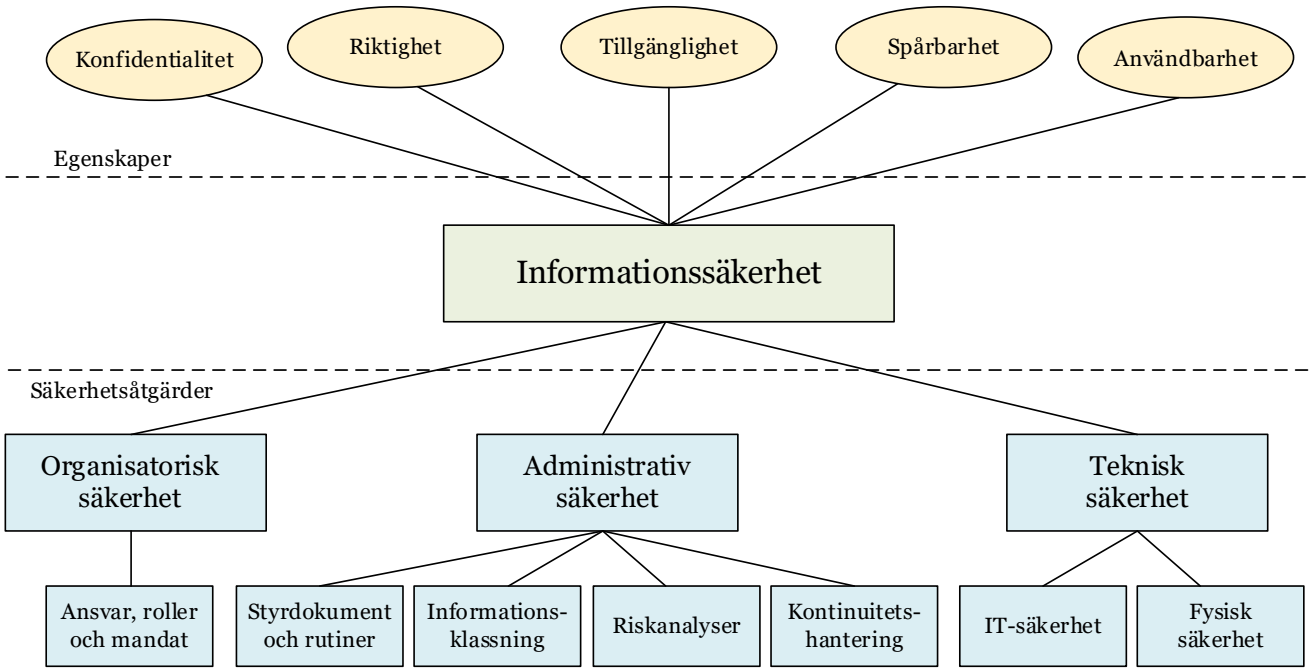
Informationssäkerhetspolicy

1 Inledning

Information är en värdefull tillgång för högskolan och högskolans verksamhet bygger i hög grad på informationshantering. Högskolans informationssäkerhetsarbete ska bedrivas på ett systematiskt, strukturerat och riskbaserat sätt i enligt med säkerhetspolicyn samt ta sin utgångspunkt i gällande lagar som t.ex. dataskyddsförordningen, MSB:s föreskrifter samt aktuell version av den internationella ledningssystemstandarden för informationssäkerhet, SS-ISO/IEC 27001.

Det övergripande syftet med högskolans informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för högskolans informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

Policyn omfattar alla informationstillgångar[1] inom verksamheten, oavsett om den behandlas manuellt eller automatiskt, och oberoende av i vilken form eller miljö den förekommer. All information ska vara klassificerad med avseende på känslighetsgrad.



Figur 1, Informationssäkerhetsmodell

Figur 1, som är baserad på informationssäkerhetsmodellen i SIS-TR 50:2015, visar en illustration över hur informationssäkerhet relaterar till informationstillgångens egenskaper samt vilka säkerhetsåtgärder som behöver tas i beaktande för att uppnå informationssäkerhet.

Organisatorisk säkerhet innebär att man fördelar ansvar, roller och mandat i organisationen för att informationen ska få nödvändigt skydd.

[1] *Informationstillgång: all information som är av värde för en organisation*

I den administrativa säkerheten inkluderas ett systematiskt arbete med att upprätta styrdokument, utforma rutiner, övervaka efterlevnad samt genomföra uppföljningar.

Nödvändiga verktyg för att uppnå adekvat informationssäkerhet är informationsklassningar, riskanalyser och kontinuitetshantering.

IT-säkerhet består av datasäkerhet som innebär skydd av data och informationssystem samt kommunikationssäkerhet som innebär skydd vid överföring av data. Exempel på datasäkerhet är behörighetskontroll, virusskydd och loggar. Exempel på kommunikationssäkerhet är VPN-lösning och separation av nätverk.

Fysisk säkerhet är en del inom informationssäkerhet som handlar om skyddsåtgärder utanför datasystemen för att undvika och förebygga fysiska hot. Fysisk säkerhet handlar om hur informationen och dess resurser behöver skyddas med hjälp av fysiska säkerhetsåtgärder som t.ex. skalskydd, lås, larm, säkra förvaringslösningar och brandskydd. Fysisk säkerhet är ett eget säkerhetsområde som inte enbart relaterar till informationssäkerhet.

2 Grundläggande principer för informationssäkerhet

Informationssäkerhet handlar om att skydda information från olika typer av hot genom att anpassa de tekniska, fysiska och administrativa miljöerna där informationen hanteras. Högskolan har ett generellt ansvar att – utifrån informationens känslighet och de risker som finns med hanteringen – genomföra lämpliga organisatoriska, administrativa och tekniska skyddsåtgärder för att säkerställa och kunna visa att hanteringen av informationen sker på lämpligt sätt och i enlighet med gällande lagstiftning.

Informationssäkerhetsarbetet ska ta sin utgångspunkt i regelbundna riskanalyser som syftar till att avväga rätt skyddsnivå i alla delar av verksamheten, samt motivera investeringar eller utbildningsinsatser för att:

- förhindra eller försvåra för obehöriga att få tillgång till information – konfidentialitet
- säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig - riktighet
- bidra till att informationen är åtkomlig för behörig person vid rätt tillfälle – tillgänglighet

Utöver dessa tre punkter är spårbarhet en stödjande och kontrollerande funktion för att säkerställa att informationens skydd upprätthålls, till exempel att den inte har ändrats, eftersökts eller lämnats ut till obehörig.

I informationssäkerhetsarbetet har även perspektivet användbarhet över tid införlivats, det vill säga att informationen ska vara läs- och tolkningsbar så länge som informationen behöver vara tillgänglig utifrån verksamhetens behov och gällande lagstiftning.

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska säkerhetsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att en tillfredsställande skyddsnivå uppnåtts.

Informationstillgångar ska som huvudregel endast hanteras i de system och tjänster som högskolan har införskaffat och som har för ändamålet anpassade lämpliga organisatoriska, administrativa och tekniska säkerhetsåtgärder.

2.1 Ledningssystem för informationssäkerhet (LIS)

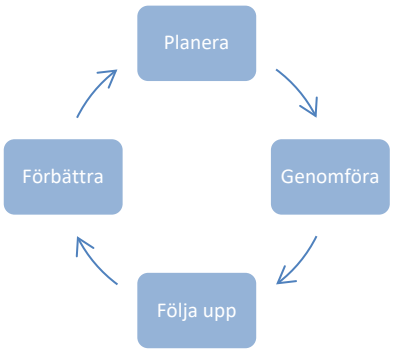
Ledningssystemet är ett verktyg för högskolans ledning att styra så att myndighetens informationshantering sker med den säkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Styrningen omfattar att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.

Ett LIS består av beslutade styrdokument med tillhörande rutiner, personella och tekniska resurser och aktiviteter för hantering av informationssäkerheten inom en organisation och syftar till att skydda högskolans informationstillgångar. Högskolans LIS dokumenteras i denna policy samt i riktlinjer, rutiner och instruktioner ordnade i en hierarkisk struktur. Ledningssystemets dokumentation ska ses som en helhet och det ska finnas en spårbarhet mellan olika ingående dokument.

Ledningssystemets viktigaste del är en säkerhetskultur som uppmuntrar medarbetarna att aktivt engagera sig i myndighetens säkerhetsarbete. Därför är ledningens engagemang liksom medarbetarnas kunskap, medvetenhet och motivation viktiga faktorer i högskolans ledningssystem.

2.1.1 Förvaltning, uppföljning och utvärdering

PDCA-modellen ("Plan-Do-Check-Act"), ska användas för att strukturera alla processer för LIS. Verksamhetens informationssäkerhetskrav och förväntningar ska på ett effektivt sätt, omhändertas och ge utfall i säker informationshantering.



Figur 2, PDCA-modellen

Planera ("Plan''), etablera och hantera policy, mål, processer och styrande dokument som är relevanta för LIS

- Högskolans informationssäkerhetspolicy ska uppfylla externa krav och organisationens behov med avseende på dess verksamhet samt kort- och långsiktiga mål.
- All information och informationshantering ska vara kopplad till en ägare (informationsägare) med en tydlig ansvarsfördelning.
- Målbilden ska vara att högskolans informationssäkerhetsrisker identifieras, analyseras och hanteras i enlighet med identifierade verksamhets- och författningskrav.

Genomföra (”Do”), driva och tillämpa säkerhetsåtgärder, processer och styrande dokument för LIS

- Formulera och genomföra planer som anger lämpliga och proportionerliga aktiviteter, resurser, ansvar och prioriteringar för att hantera informationssäkerhetsrisker både på kort och lång sikt.

Följa upp (”Check”), granska och mäta processers effektivitet i förhållande till policy, mål och praktisk erfarenhet samt rapportera till ledningen för återkoppling och fastställande om fortsatt inriktning.

- Genomföra regelbundna granskningar av LIS effekt med hänsyn till efterlevnad, revisioner, incidenter, förslag och återkoppling ifrån verksamheten.
- Granska informationsklassningar och riskanalyser regelbundet för att kontrollera kvarvarande risker med hänsyn till förändringar i verksamhet, skyddsteknik, hotbild och författningar/regelverk.
- Regelbundet genomföra genomgång av LIS för ledningen för att säkerställa korrekt omfattning och att lämpliga förbättringar av LIS identifieras.

Förbättra (”Act”), vidta korrigerande och förbättrande åtgärder, baserade på resultaten av interna revisioner av LIS och ledningens genomgång eller annan relevant information, för att ständigt förbättra LIS.

- Genomföra identifierade förbättringsåtgärder av LIS.
- Säkerställa att LIS har följsamhet gentemot författningsändringar, externa krav och erfarenheter ifrån andra organisationer.

2.1.2 Informationsklassning

Informationsklassning ska vara en central aktivitet i informationssäkerhetsarbetet och har till syfte att bedöma informationens värde för högskolans verksamhet. Bedömning sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd.

Informationsklassningen är en process som innebär en kravställning på säkerhetsåtgärder från verksamheten till interna och externa leverantörer av tjänster samt IT (drift och förvaltning) och av resurser som lokaler och annan utrustning som påverkar informationshanteringen. Klassningen innebär även krav på användare av informationstillgångar. Informationsklassning ska ses som en form av riskanalys som gäller specifika informationstillgångar.

För att klassningen ska medföra en säkerhetshöjande effekt krävs att det finns systematiserade skyddsåtgärder som hanterar riskerna.

2.1.3 Riskanalyser

Riskanalys innebär att definiera de hot som är riktade mot en verksamhet eller mot en informationstillgång samt sannolikheten för att de inträffar. Analysen innehåller en värdering av konsekvenserna av ett förverkligat hot. Lämpligt val av skyddsåtgärder görs utifrån sannolikhet och konsekvens.

2.1.4 Kontinuitetshantering

Kontinuitetshantering avser förmågan att reducera negativa effekter i verksamheten orsakade av olika former av störningar i tillgång till information.

Kontinuitetshanteringen ur informationssäkerhetsperspektivet ska riktas mot att reducera avbrott och allvarliga störningar som påverkar informationshanteringen och därmed skapar störningar i verksamheten oavsett var de uppstår. Incidenten kan ha sitt ursprung i exempelvis en brand eller ett inbrott men få påverkan på informationshanteringen. Störningarna kan vara av olika karaktär, allt från mindre störningar till katastroftillstånd. Avsikten är att verksamhetsprocesserna så snabbt som möjligt efter en störning kan återgå till normalläge och att minimera risken för informationsförluster under störningen. För att uppnå detta måste kontinuitetshanteringen, ur informationssäkerhets-synpunkt, integreras med högskolans ordinarie riskhanteringsarbete.

Kontinuitetshanteringen ur informationssäkerhetssynpunkt innehåller dels den kontinuitets-hanteringen som verksamheten har ansvar för, dels den avbrottsplanering som IT-avdelningen och andra teknikresursägare ska ha för att kunna leverera stöd till verksamheten. Kontinuitetshantering ska finnas för varje verksamhet samt för stödfunktioner, t.ex. IT-avdelningens plan ska utformas efter de krav som verksamheten formulerar. Planerna ska finnas tillgängliga för behöriga medarbetare och förvaras och hanteras utifrån kravställning enligt genomförd informationsklassning.

2.1.5 Incidenthantering

En väl fungerande hantering av säkerhetsincidenter är en mycket viktig del av både det reaktiva och proaktiva säkerhetsarbetet. Det ger dels möjlighet att snabbt och effektivt agera på uppkomna hot och händelser, dels möjlighet att i efterhand vidta förebyggande åtgärder för att motverka att liknande incidenter inträffar på nytt. En grundläggande förutsättning för att detta ska fungera är att samtliga verksamma vid högskolan har kunskap om vad som definieras som en incident, samt var och hur dessa ska anmälas internt inom organisationen.

3 Ansvar och roller för arbetet

Ansvaret för informationssäkerhet uppdelas i ledningsansvar och verksamhetsansvar (Ansvar och roller i ledningssystem för informationssäkerhet vid Högskolan i Borås, dnr 151-22). Det är högskolans ledning som med hjälp av LIS styr så att myndighetens informationshantering sker med adekvat säkerhet utifrån verksamhetens behov och externa krav. Verksamheten ska tillämpa de av ledningen beslutade åtgärderna för att uppnå lämplig organisatorisk och teknisk säkerhetsnivå vid all informationshantering.

4 Revidering, uppföljning och information

Enligt SS-ISO/IEC 27001 och MSB:s föreskrifter om informationssäkerhet för statliga myndigheter ska varje myndighet minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning. Vid Högskolan i Borås ska styrelsen och ledningsgruppen minst en gång per år informeras om i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov, allvarliga risker som inte åtgärdats, och övriga hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet.