Informationssäkerhetspolicy vid Karlstads universitet

1 Inledning

Information är en värdefull tillgång i Karlstads universitets verksamhet, både i det dagliga arbete och på längre sikt. Karlstads universitets verksamhet bygger i hög grad på informationshantering.

Informationssäkerhet handlar om hur informationen ska skyddas. Informationssäkerhet är teknikneutralt och omfattar skydd av alla former av information, oavsett om den finns i exempelvis IT-system, på papper eller förekommer under samtal.

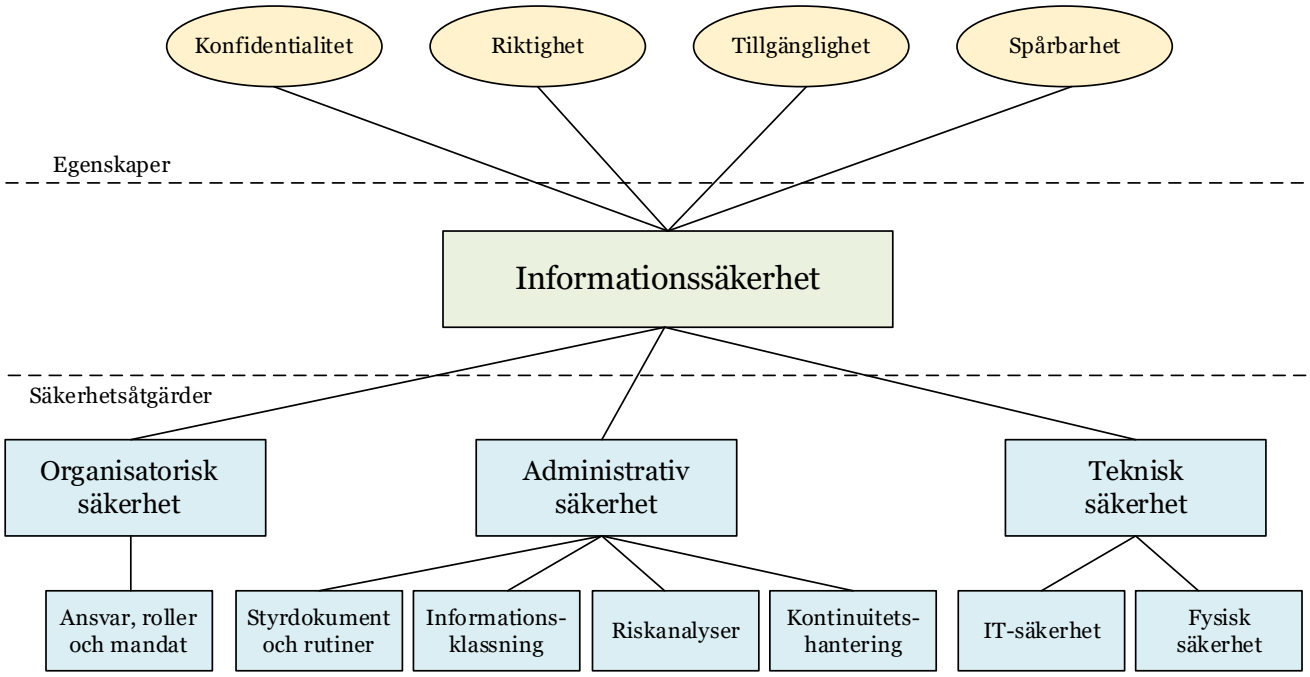
Karlstads universitets informationssäkerhetsarbete ska bedrivas på ett systematiskt, formaliserat och riskorienterat sätt och ta sin utgångspunkt i gällande lagar, förordningar och föreskrifter som till exempel dataskyddsförordningen och MSB:s föreskrifter, samt aktuell version av den internationella ledningssystemstandarden för informationssäkerhet, SS-ISO/IEC 27001.

Det övergripande syftet med Karlstads universitets informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för universitetets informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt.

Policyn omfattar alla informationstillgångar inom verksamheten utan undantag, 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.

Karlstads universitet
651 88 Karlstad
Tfn 054-700 10 00
Fax 054-700 14 60
Information@kau.se

Beslut:	109/21	Dnr:	C2021/960	Ersätter:	RB 46/17	Dnr:	C2017/287
Giltighet fr.o.m:	2021-11-15	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		



Figur 1, Informationssäkerhetsmodell.

Figur 1, som är baserad på informationssäkerhetsmodellen i SIS-TR 50:2015[1], 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.

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 även fortlöpande informationsklassningar, riskanalyser och kontinuitetshantering.

IT-säkerhet består av datasäkerhet som innebär skydd av data och informationssystem, och 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 mekanism inom informationssäkerhet som handlar om skyddsåtgärder utanför datasystemen för att undvika och förebygga fysiska hot. Fysiska hot kan orsakas av exempelvis strömförsörjning, naturkatastrofer och mänsklig åverkan. Fysisk säkerhet handlar om hur informationen och dess resurser behöver skyddas med hjälp av fysiska säkerhetsåtgärder som till exempel skalskydd, lås, larm, säkra förvaringslösningar och brandskydd. Fysisk säkerhet är också ett eget säkerhetsområde som inte enbart relaterar till informationssäkerhet.

[1] Termer, definitioner och förklaringar är återgivna ur SIS Tekniska rapport, Terminologi för informationssäkerhet, utgåva 1, med vederbörligt tillstånd från SIS Förlag AB.

2 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015 eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges.

Administrativ säkerhet (inom ramen för ledningssystem för informationssäkerhet, LIS, vid Karlstads universitet): säkerhetsåtgärder relaterade till hur verksamheten styr informationssäkerhetsarbetet i en organisation.

Fysik säkerhet: tekniska säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten. Fysisk säkerhet är också ett eget säkerhetsområde som inte enbart relaterar till informationssäkerhet.

Hot: möjlig, oönskad händelse med negativa konsekvenser för verksamheten.

Information: innebörd i data.

Informationsbehandlingsresurs: system, tjänst eller infrastruktur för hantering av information eller de fysiska platser där dessa finns.

Informationshantering (inom ramen för LIS vid Karlstads universitet): insamling, behandling, lagring och överföring av information så att informationen kan användas på ett ändamålsenligt och kontrollerat sätt.

Informationssystem: applikationer, tjänster eller andra komponenter som hanterar information.

Informationssäkerhet: bevarandet av konfidentialitet, riktighet och tillgänglighet hos information.

Informationstillgång: all information som är av värde för en organisation.

IT-säkerhet: IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet.

LIS: ledningssystem för informationssäkerhet.

Organisatorisk säkerhet (inom ramen för LIS vid Karlstads universitet): roller och ansvarsfördelning för att uppnå informationssäkerhet.

Säkerhetsåtgärd: åtgärd som förändrar en risk. Säkerhetsåtgärder inkluderar varje process, policy, utrustning, praxis eller annan åtgärd som förändrar en risk.

Teknisk säkerhet (inom ramen för LIS vid Karlstads universitet): tekniska säkerhetsåtgärder för att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet.

3 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. Karlstads universitet har ett generellt ansvar att – utifrån informationens känslighet och de risker som finns med hanteringen – genomföra lämpliga tekniska och organisatoriska skyddsåtgärder för att säkerställa och kunna visa att hanteringen av informationen sker på lämpligt sätt och i enlighet med gällande lagar, förordningar och föreskrifter.

Informationssäkerhetsarbetet ska ta sin utgångspunkt i informationsklassning och 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.

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska skyddsåtgärder 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 informationsbehandlingsresurser som Karlstads universitet har införskaffat och som har för ändamålet anpassade lämpliga tekniska och organisatoriska skyddsåtgärder.

3.1 Ledningssystem för informationssäkerhet (LIS)

Ledningssystemet är ett verktyg för Karlstads universitets 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.

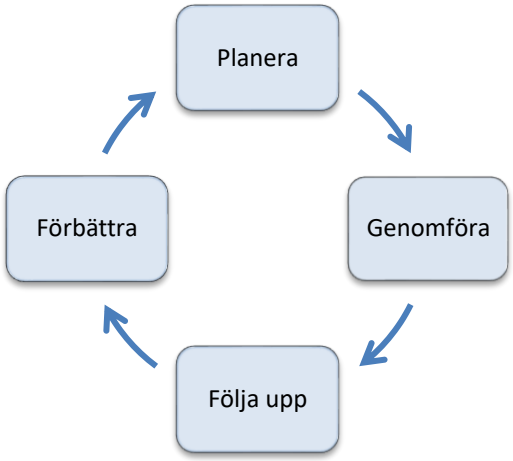
Ett LIS består av beslutade styrdokument med tillhörande rutiner, personella och tekniska resurser, och aktiviteter för hantering av informationssäkerheten inom en organisation. Denna hantering syftar till att skydda universitetets informationstillgångar. Karlstads universitets LIS dokumenteras i denna 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 positiv informationssäkerhetskultur som uppmuntrar medarbetarna att aktivt engagera sig i myndighetens informationssäkerhetsarbete. Att ha en bra informationssäkerhetskultur innebär att alla på arbetsplatsen är medvetna om de risker som finns och har både kunskap och vilja att minska dem. Det gäller att skapa ett arbetssätt där informationssäkerhet är en självklar del i verksamhetens arbete. Därför är ledningens engagemang liksom medarbetarnas kunskap, medvetenhet och motivation viktiga faktorer i universitetets ledningssystem.

3.1.1 Förvaltning, uppföljning och utvärdering

PDCA-modellen ("Plan-Do-Check-Act"),

Figur 2, 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

- Karlstads universitets informationssäkerhetspolicy ska motsvara organisationens behov med avseende på dess verksamhet samt kort- och långsiktiga mål.
- Målbilden ska vara att Karlstads universitets 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 på lång sikt.
- All information och informationshantering ska vara kopplad till en ägare med tydlig ansvarsfördelning.

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 ledningens genomgång av LIS 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.

3.2 Informationsklassning

Informationsklassning ska vara en central aktivitet i informationssäkerhetsarbetet och har till syfte att bedöma informationens värde för myndighetens 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.

3.3 Riskanalyser

Riskanalys ska användas för att identifiera de hot som är riktade mot en verksamhet eller mot en informationstillgång samt sannolikheten för att de förverkligas. Analysen innehåller en värdering av konsekvenserna av ett förverkligat hot. Därefter kan ett lämpligt val av skyddsåtgärder göras.

3.4 Kontinuitetshantering

Kontinuitetshantering ska användas för att reducera negativa effekter i verksamheten orsakade av olika former av störningar i tillgång till information.

Kontinuitetshanteringen ur informationssäkerhetsperspektivet ska riktas mot 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 inga väsentliga informationsförluster sker under störningen.

För att detta ska kunna uppnås måste kontinuitetshantering ur informationssäkerhetssynpunkt integreras med Karlstads universitets ordinarie riskhanteringsarbete. Detta innebär bland annat att det ska finnas beskrivet vilka risker som Karlstads universitet är utsatt för.

Kontinuitetshanteringen ur informationssäkerhetssynpunkt innehåller dels den egentliga kontinuitetshanteringen 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, till exempel IT-avdelningens plan som ska utformas efter de krav som verksamheten formulerar.

Planerna ska finnas tillgängliga för behöriga medarbetare och förvaras och hanteras utifrån kravställning enligt genomförd informationsklassning.

3.5 Incidenthantering

Incidenthantering ska vara en del av både det reaktiva och proaktiva säkerhetsarbetet. Det ger dels möjlighet att snabbt och effektivt agera på uppkomna hot och händelser, och 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 Karlstads universitet har kunskap om vad som definieras som en incident, samt var och hur dessa ska anmälas internt inom organisationen.

4 Ansvar och roller

Ansvaret för informationssäkerhet uppdelas i ledningsansvar och verksamhetsansvar. Det är Karlstads universitets 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.

5 Uppföljning

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 Karlstads universitet ska universitetsstyrelsen årligen 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.