Riktlinjer för ansvar och roller i ledningssystem för informationssäkerhet (LIS) vid Karlstads universitet

1 Inledning

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.

2 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015[1] eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges. För ytterligare definitioner se Karlstads universitets informationssäkerhetspolicy.

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.

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.

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.

Konsekvensnivå: en beskrivning av hur allvarlig konsekvensen riskerar att bli om ett hot inträffar.

Säkerhetsåtgärder: identifierad uppsättning åtgärder för att möta en organisations risker.

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

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

Beslut:	110/21	Dnr:	C2021/961	Ersätter:	-	Dnr:	-
Giltighet fr.o.m:	2021-11-15	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

Skyddsnivå: ett antal samlade säkerhetsåtgärder som ger tillräckligt skydd för information som klassats till en viss konsekvensnivå. Definierat i MSB:s metodstöd[2] för informationssäkerhet.

3 Ledningsansvar

Arbetet med informationssäkerhet i en organisation förutsätter att ledningen har en förståelse för de risker som organisationens informationshantering är utsatt för och hur de kan hota verksamheten. Utifrån ett systematiskt informationssäkerhetsarbete behöver ledningen säkerställa att det finns tillräckliga administrativa och tekniska resurser för att reducera risker och skapa kvalitetshöjande effekter.

3.1 Rektor

Rektor har som myndighetschef huvudansvaret för att säkerställa att verksamheten bedrivs författningsenligt och effektivt. Rektor har det yttersta ansvaret för det strategiska informationssäkerhetsarbetet vid Karlstads universitet. I detta ingår bland annat att fatta beslut om policy och riktlinjer, samt säkerställa att det på universitetsövergripande nivå finns resurser för att genomföra det som förskrifter och internt beslutade regler föreskriver. I ansvaret ingår även att fatta beslut beträffande hantering av identifierade risker som kan få mycket allvarliga konsekvenser för hela myndighetens verksamhet.

3.2 Universitetsdirektör

Universitetsdirektören beslutar om det övergripande systematiska informationssäkerhetsarbetet vid Karlstads universitet i övrigt och är direkt underställd rektor.

På Centrala stödfunktioner är det universitetsdirektören som har det övergripande ledningsansvaret för Centrala stödfunktioners informationssäkerhetsarbete. Detta ledningsansvar innefattar bland annat att ha en uppdaterad lägesbild över identifierade risker som kan få allvarliga konsekvenser för Centrala stödfunktioners verksamhet och besluta hur dessa risker ska hanteras.

3.3 Chef för rektors kansli

Chefen för rektors kansli, som är direkt underställd universitetsdirektören, har ansvar för utveckling och införande av det systematiska informationssäkerhetsarbetet vid Karlstads universitet.

3.4 Dekaner

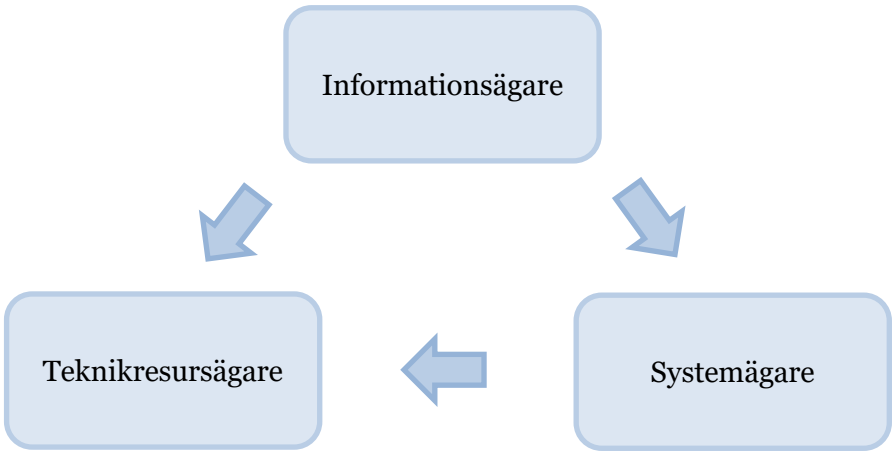
På fakultetsnivå är det dekanen som har det övergripande ledningsansvaret för fakultetens informationssäkerhetsarbete. Detta ledningsansvar innefattar bland annat att ha en uppdaterad lägesbild över identifierade risker som kan få allvarliga konsekvenser för fakultetens verksamhet och besluta hur dessa risker ska hanteras.

4 Verksamhetsansvar

Verksamhetsansvaret för informationssäkerheten vid Karlstads universitet är uppbyggt kring samverkan mellan informationsägare, systemägare och

[2] https://www.informationssakerhet.se

teknikresursägare, se Figur 1. Dessa olika roller kan beroende på den aktuella situationen innehas av en enda person eller av flera olika personer.



Figur 1, När informationen hanteras i IT-system och IT-tjänster ställer informationsägaren som huvudregel sina krav till systemägaren, som i sin tur kan ställa ytterligare krav till teknikresursägaren. När informationen hanteras på övriga IT-resurser, som till exempel USB-minnen och diktafoner, eller på fysiskt medium, som till exempel pappersdokument, ställer informationsägare sina krav direkt till teknikresursägaren. Beroende på situationen kan en person inneha en, två eller samtliga roller (informationsägare, systemägare och teknikresursägare).

I verksamhetsansvaret ingår bland annat att upprätta nödvändiga administrativa rutiner och instruktioner för hantering av informationstillgångar. Aktiviteterna som följer av ledningssystemet ska ingå i den ordinarie verksamhetsplaneringen för dessa roller.

Alla identifierade risker ska prioriteras och hanteras. Kvarvarande risker som kan få allvarliga konsekvenser för verksamheten ska hanteras i samråd med närmsta chef.

4.1 Informationsägare

Alla informationstillgångar ska identifieras och inordnas under en informationsägare. Informationsägaren ansvarar för att säkerställa att informationstillgången klassificeras enligt kriterierna konfidentialitet, riktighet och tillgänglighet, i syfte att precisera skyddsbehov utifrån verksamhetens beroende till informationen. Genom att tillämpa universitetets metodstöd för informationsklassning och skyddsnivåer bestäms också vilka tillgångar som är verksamhetskritiska för att kunna prioritera införandet av lämpliga skyddsåtgärder.

Eftersom skadeverkningarna av bristande säkerhet i system och tjänster uppstår inom informationsägarens verksamhet är det informationsägaren som ska säkerställa att risker bedöms och adekvata säkerhetskrav ställs med stöd av genomförd informationsklassning.

Rollen som informationsägare innebär ett ansvar och ett förvaltarskap för den information som skapas och hanteras inom de processer som ingår i den egna verksamheten. I detta ansvar ingår att säkerställa att lämpligt skydd för informationstillgångarna upprättas och vidmakthålls i enlighet med exempelvis dataskyddslagstiftning, arkivlagstiftning och föreskrifter från MSB. Rollen innehas främst av prefekt, föreståndare för forskningscentrum eller avdelningschef. Informationsägarskapet innebär ett chefsansvar på samma sätt som budget-, kvalitets- och miljöansvar.

4.2 Systemägare

Systemägaren är den som har till uppgift att se till att de system och tjänster som används i verksamheten uppfyller Karlstads universitets krav gällande informationssäkerhet och integritetsskydd vid behandling av personuppgifter. Varje system och tjänst som används för Karlstads universitets verksamhet ska ha en utsedd systemägare. Rollen som systemägare motsvarar systemgruppsägare enligt Karlstads universitets förvaltningsmodell.

Rollen som systemägare innebär att vara mottagare av de krav på säkerhet som följer av informationsklassningen som genomförts av informationsägaren. Systemägaren svarar för leveransen av en tjänst eller ett system och har det ekonomiska ansvaret. Om externa system- eller tjänsteleverantörer används ska systemägaren inom Karlstads universitet säkerställa att säkerhetskraven ställs, uppfylls och följs upp.

4.3 Teknikresursägare

Rollen som teknikresursägare innebär att vara ägare av resurser som används för Karlstads universitets informationshantering. Detta omfattar interna och externa IT-resurser samt även lokaler. Teknikresursägaren kan vara antingen intern på Karlstads universitet eller en extern leverantör. I ansvaret ligger att tillse att resursen har rätt säkerhetsnivå utifrån systemägarens eller informationsägarens krav.

4.3.1 IT-infrastrukturägare

IT-infrastrukturägare ska finnas för alla resurser, som till exempel nät, servrar och annan hårdvara. Det är IT-infrastukturägaren som ansvarar för att IT-säkerhetskraven som ställs av systemägaren eller informationsägaren uppfylls. Rollen som IT-infrastrukturägare motsvarar IT-ägare enligt Karlstads universitets förvaltningsmodell. Vid anlitande av externa leverantörer ska adekvata säkerhetskrav alltid fastställas i avtalet med leverantören.

4.3.2 Lokalansvarig

Lokalansvarigs ansvar avgränsas till de byggnadstekniska förutsättningarna, medan utrustning med mera som nyttjas i lokalen är exempelvis IT-infrastrukturägares eller informationsägares ansvarsområde. För utformning av fysiskt skydd för olika typer av lokaler, gemensamma såväl som verksamhetsspecifika, ska LIS anvisningar för fysiskt skydd tillämpas. För att samordna användningen av resurserna ska det finnas en centralt ansvarig för Karlstads universitets lokaler. Vid Karlstads universitet innehas denna roll av avdelningschefen för Campusservice.

4.4 Övriga roller inom verksamhetsansvaret

Utöver det ansvar som tillfaller nyckelrollerna informationsägare, systemägare och teknikresursägare förutsätter ett systematiskt och effektivt informationssäkerhetsarbete att alla medarbetare verkar för en god informationssäkerhetskultur vid utförandet av sina arbetsuppgifter.

4.4.1 Chefer

Respektive chef ansvarar för att samtliga medarbetare inom sitt ansvarsområde får lämplig utbildning inom informationssäkerhet. Medarbetare med ansvar för vitala resurser som exempelvis brandväggar, nätverk, datorhallar och arkiv ska ges särskild utbildning i säkerhetsfrågor.

4.4.2 Medarbetare och konsulter

Alla medarbetare ska följa Karlstads universitets säkerhetsregler och ta del av informations- och utbildningsinsatser inom informationssäkerhetsområdet. Medarbetare ska också vara medvetna om Karlstads universitets inriktning för god informationssäkerhet, de säkerhetsrisker som kan finnas i det dagliga arbetet och verka för en god informationssäkerhetskultur.

Även extern personal som till exempel konsulter ska ta del av och följa universitetets säkerhetsregler.

4.4.3 Ansvar för informationssäkerhet i projekt

Ansvar för informationssäkerheten i exempelvis forskningsprojekt eller IT-projekt som påverkar Karlstads universitets informationshantering ligger dels hos informationsägaren, dels hos projektledaren. Informationsägaren, vanligen prefekt, föreståndare för forskningscentrum eller avdelningschef, ska beskriva de övergripande säkerhetskrav som finns för projekten, samt avsätta tillräckliga personella och ekonomiska resurser för säkerställande av kravbilden. Projektledaren har ansvar för att en informationsklassning görs enligt Karlstads universitets modell för informationsklassning. Dessutom ska projektledare, med stöd av expertfunktioner, genomföra nödvändiga riskanalyser där den tänkta informationshanteringen ska beakta informationssäkerheten.

5 Övriga nyckelroller och funktioner

Vid Karlstads universitet finns ett antal övriga nyckelroller och funktioner som stödjer verksamhetens informationssäkerhetsarbete.

5.1 Informationssäkerhetsansvarig

Informationssäkerhetsansvarig stödjer universitetets ledning i det systematiska och operativa arbetet med informationssäkerhet inom Karlstads universitet.

Ansvaret för informationssäkerhetsansvarig omfattar bland annat följande punkter:

- Besluta om instruktioner och lathundar för hur informationssäkerhetsarbetet ska bedrivas.
- Rapportera till ledningen i informationssäkerhetsfrågor i enlighet med MSB:s föreskrifter.
    - Rapport en gång per år till universitetsstyrelsen.
    - Rapport en gång i kvartalet till universitetsdirektören.
    - Rapport av allvarliga brister till universitetsdirektör och rektor så snart som möjligt.
- Utgöra ett stöd till organisationen i informationssäkerhetsfrågor.
- Slutrapportera IT-incidenter till MSB.
- Årligen sammanställa incidenter inom informationssäkerhetsområdet.
- Årligen granska kontinuitetshanteringen.
- Säkerställa adekvat omvärldsbevakning inom informationssäkerhet.

- Initiera och genomföra revisioner och kontroller av informationssäkerheten.
- Ta fram informations- och utbildningsmaterial rörande informationssäkerhet samt genomföra utbildningar för olika grupper.

5.2 Säkerhetschef

Säkerhetschefen stödjer universitetets ledning i det systematiska och operativa arbetet med fysisk säkerhet inom Karlstads universitet, och har ett övergripande ansvar för fysisk säkerhet. Som stöd i sitt arbete har säkerhetschefen en säkerhetskoordinator.

Ansvaret för säkerhetschefen omfattar bland annat följande punkter som berör informationssäkerhet:

- Ta fram universitetsövergripande styrdokument för hur det fysiska säkerhetsarbetet ska bedrivas som beslutas av rektor.
- Ta fram och besluta instruktioner och lathundar för hur det fysiska säkerhetsarbetet ska bedrivas.
- Ta fram och besluta skyddsnivåer för fysisk säkerhet.
- Ansvara för universitetets krisorganisation.
- Ansvara för det övergripande och organisatoriska arbetet med säkerhetsincidenter.
- Rapportera till ledningen i fysiska säkerhetsfrågor.
    - Rapport en gång per år till universitetsstyrelsen.
    - Rapport en gång i kvartalet till universitetsdirektören.
    - Rapport av allvarliga brister till universitetsdirektör och rektor så snart som möjligt.
- Utgöra ett stöd till organisationen i fysiska säkerhetsfrågor.
- Årligen sammanställa incidenter inom fysiska säkerhetsområdet.
- Säkerställa adekvat omvärldsbevakning inom fysisk säkerhet.
- Initiera och genomföra revisioner och kontroller av den fysiska säkerheten.
- Ta fram informations- och utbildningsmaterial rörande fysisk säkerhet samt genomföra utbildningar för olika grupper.

5.3 IT-chef

IT-chefen är den som ansvarar för Karlstads universitets IT-säkerhet och ska vidta lämpliga IT-säkerhetsåtgärder. IT-säkerhet är därmed en del i IT-chefens generella chefsansvar och ska ingå i den ordinarie verksamhetsplaneringen.

Ansvaret omfattar bland annat följande punkter:

- Säkerställa att föreskrifter om IT-säkerhet uppfylls.
- Ta fram och besluta skyddsnivåer som berör IT-säkerhet.
- Upprätta en företeckning av hur Karlstads universitets IT-systems och IT-tjänsters uppfyller myndighetens skyddsnivåer som berör IT-säkerhet.
- Ta fram universitetsövergripande styrdokument avseende IT-säkerhet som beslutas av rektor.
- Ta fram och besluta om interna rutiner avseende IT-säkerhet för Karlstads universitet.
- Säkerställa adekvat omvärldsbevakning inom IT-säkerhet.
- Stödja systemägaren vid anskaffning av externa system och tjänster med att säkerställa att IT-säkerhetskraven ställs, uppfylls och följs upp.
- Utse en person som har uppdraget IT-säkerhetssamordnare för att utveckla och förvalta IT-säkerheten, samt tillse att denne får tillräckliga resurser för att genomföra arbetet.

5.4 IT-säkerhetssamordnare

IT-säkerhetssamordnare svarar under IT-chefen för IT-säkerhetsarbetet vid Karlstads universitet och stödjer dessutom informationssäkerhetsarbetet genom att identifiera lämpliga tekniska lösningar på de funktionella krav som ställs i ledningssystemet. Särskild hänsyn ska tas till de krav som ställs i dataskyddsförordningen samt MSB:s föreskrifter.

IT-säkerhetssamordnare ska stödja universitetet i planering, genomförande och uppföljning av IT-säkerhetsarbetet. Ansvaret omfattar bland annat följande punkter

- Ta fram strategiska underlag i IT-säkerhetsfrågor utifrån en kontinuerlig omvärldsbevakning.
- Vara IT-avdelnings kontaktperson i IT-säkerhetsfrågor.
- Medverka i upphandlingar och projekt som påverkar informationssäkerheten.
- Stödja universitetet i riskanalyser.
- Utgöra ett stöd för universitetet i de aktiviteter som följer av LIS.
- Årligen sammanställa IT-incidenter och rapportera dessa till informationssäkerhetsansvarig.
- Initiera och genomföra revisioner och kontroller av IT-säkerheten inom Karlstads universitet.

5.5 Informationshanteringsrådet

Vid Karlstads universitet finns ett informationshanteringsråd som stödjer verksamheten i frågor om informationshantering, inklusive arkiv och registratur, informationssäkerhet och integritetsskydd. Informationshanteringsrådet har bland annat följande uppgifter inom informationssäkerhet.

- Ta fram universitetsövergripande styrdokument för hur informationssäkerhetsarbetet ska bedrivas som beslutas av rektor.
- Ta fram instruktioner och lathundar för hur informationssäkerhetsarbetet ska bedrivas som beslutas av informationssäkerhetsansvarig.
- Stödja arbetet med omvärldsbevakning inom informationssäkerhet.

5.6 Säkerhetsgruppen

På Karlstads universitet finns en säkerhetsgrupp som består av säkerhetschefen, säkerhetskoordinatorn, informationssäkerhetsansvarig, IT-säkerhetssamordnare och dataskyddsombudet. Säkerhetsgruppen arbetar operativt med universitets säkerhetsfrågor. Säkerhetsgruppen har även till uppgift att informera och levandegöra säkerhetsfrågorna i verksamheten, och ska se till att berörda målgrupper kan hålla sig uppdaterade och får möjlighet till regelbunden utbildning.

5.7 Expertfunktioner

Informationssäkerhetsansvarig, arkivarie, dataskyddsombud, universitetsjurist, IT-strateg, förvaltningsledare, IT-säkerhetssamordnare, säkerhetsfunktionen med flera ska delta aktivt i det operativa arbetet, till exempel delge sin expertkunskap vid genomförande av informationsklassning och riskanalys.