Riktlinjer för roller och ansvar inom ledningssystem för informationssäkerhet vid Karolinska Institutet

Dnr 1-141/2025

Gäller fr.o.m. 2025-06-05

Karolinska Institutet

Riktlinjer för roller och ansvar inom ledningssystem för informationssäkerhet vid Karolinska Institutet

Innehåll

Diarienummer	Dnr föreg. version:	Beslutsdatum:	Giltighetstid:
Dnr 1-141/2025	Dnr 1-393/2019	2025-06-05	Fr.o.m. 2025-06-05 och tills vidare

Beslut:
Universitetsdirektören

Dokumenttyp:
Riktlinjer

Handläggs av avdelning/enhet:
Avdelningen för juridik, planering och ekonomi

Beredning med:
Avdelningen för forskarstöd och externa relationer, IT-avdelningen

Revidering med avseende på:
Nytt styrdokument som ersätter tidigare riktlinjer med ändring på struktur och innehåll.

1. Inledning

Karolinska Institutet (KI) hanterar stora mängder känslig information inom sin forskning och utbildning vilket ställer krav på en väl avvägd och ändamålsenlig informationssäkerhetsnivå. Därför behöver informations-säkerhetsaspekterna vara en integrerad del i den ordinarie verksamheten och vägas in i de beslut som fattas.

Informationssäkerhetsarbetet ska vara till skydd för KI:s öppna samarbetsinriktade miljö.

1.1 Syfte

Syftet med riktlinjerna är att tydliggöra hur olika roller berörs av informationssäkerhetsfrågorna genom vägledning kring vad som kan vara lämpligt i olika situationer men även genom att ange vilka regler man behöver följa inom KI.

Riktlinjerna utgår från KI:s informationssäkerhetspolicy och kompletteras med vägledningar och metodstöd.

Grund för riktlinjerna är informationssäkerhetsstandarden SS-EN ISO/IEC 27002:2022 samt Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2020:6), föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7) samt föreskrifter om rapportering av IT-incidenter för statliga myndigheter (MSBFS 2020:8).

1.2 Definitioner

Informationstillgångar: Information lagrad och kommunicerad i alla former, elektronisk, pappersbaserad, muntlig samt tekniska tillämpningar för informationshantering i form av t.ex. hård-, mjukvara och tjänster.

Verksamhetskritisk information: Information som t.ex. har samlats in under lång tid och kan vara svår att återskapa. Informationen kan vara av stort värde t.ex. för ett forskningsprojekt, forskargrupp, institution eller hela KI.

Personuppgifter: Uppgifter som kan knytas till en identifierbar levande person.

Känsliga personuppgifter/särskilda kategorier av personuppgifter: Uppgifter som direkt eller indirekt kan knytas till en person som är i livet och som berör uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter, biometriska uppgifter.

Informationssäkerhet: Bevarande av informationens konfidentialitet (sekretess), tillgänglighet och riktighet.

Konfidentialitet (sekretess): Egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer

Riktighet: Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring

Tillgänglighet: Egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning

Risk: Osäkerhetens effekt på mål – uttrycks som en kombination av en händelses konsekvenser och tillhörande sannolikhet för att den inträffar.

IT-säkerhet: Del av informationssäkerhet avgränsad till IT-resurser - Tekniska skyddsåtgärder för att skydda t.ex. nät och servrar, VPN-förbindelser, antivirus och intrångsdetektering.

Informationssäkerhetsincident: Oönskad händelse som har inträffat och som innebär negativa konsekvenser för verksamheten och dess informationssäkerhet.

Ledningssystem för informationssäkerhet (LIS): Organisationsstruktur, policyer, planeringsaktiviteter, ansvar, praxis, rutiner, processer och resurser som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.

2. Områden

2.1 Organisation av informationssäkerhetsarbetet

Ansvaret för informationssäkerheten regleras i KI:s informationssäkerhetspolicy. Grundprincipen är att ansvaret följer det ordinarie verksamhetsansvaret.

Konsistoriet har det yttersta ansvaret för informationssäkerheten och anger principerna för arbetet i informationssäkerhetspolicyn. Konsistoriet informerar sig en till två gånger per år om hur informationssäkerhetsarbetet når målen.

Universitetsledningen främjar utvecklingen av informationssäkerhetsarbetet brett inom KI och informerar sig två till fyra gånger per år om hur befintliga säkerhetsåtgärder motsvarar behoven inom KI, om det föreligger några svårigheter med att uppnå informationssäkerhetspolicyns målsättningar och i stort huruvida informationssäkerhetsarbetet når avsett resultat.

Prefekten ansvarar för informationssäkerheten inom sin institution. En översikt bör finnas av vilken verksamhetskritisk information som hanteras, vilka tekniska lösningar för informationshantering som existerar vid sidan av de som tillhandahålls av KI:s centrala IT-avdelning, vilka risker man bedömer existera i sin informationshantering, vilka eventuella förbättringsåtgärder som är nödvändiga samt att statusen och eventuella förbättringsåtgärder utvärderas. Detta bör dokumenteras och sker lämpligen i samband med verksamhetsplanering och budgetarbete.

Verksamhetsansvariga – avdelningschef, enhetschef, forskargruppledare, FUA, GUA är operativt ansvariga för att verksamhetskritiska informationsbehandlingar dokumenteras och riskbedöms samt att nödvändiga förbättringsåtgärder genomförs inom sitt ansvarsområde.

KI:s centrala IT-avdelning har i uppdrag att tillhandahålla förutsättningar för en säker och effektiv informationshantering inom hela KI. Till stöd i arbetet finns en IT-säkerhetsansvarig. Här finns också ansvaret för att vid behov

utforma detaljerade styr- och stöddokument för IT-verksamheten baserat på KI:s informationssäkerhetspolicy och övriga styr- och stöddokument avseende informationssäkerhet.

I det fall IT-verksamhet organiseras internt inom en institution för att stödja särskilda verksamhetsspecifika behov ansvarar institutionen för en säker och effektiv informationshantering i den lokala IT-verksamheten.

Vid outsourcad informationshantering har den avtalsansvarige chefen på KI ansvaret för att informationssäkerheten förblir tillfredsställande under hela kontraktstiden.

Samtliga verksamma inom KI har ett ansvar att följa KI:s regler inom informationssäkerhetsområdet och att genomgå de säkerhetsutbildningar som erbjuds internt. Samtliga ansvarar också för att uppmärksamma och vara vaksamma på säkerhetsbrister och säkerhetsincidenter och se till att dessa rapporteras. (*Se Anvisningar om informationssäkerhet för verksamma inom KI.)*

Informationssäkerhetsfunktionen ansvarar för att långsiktigt och kontinuerligt inrikta, leda, stödja och följa upp informationssäkerhetsarbetet för KI som helhet.

Status om informationssäkerheten ska regelbundet rapporteras till universitetsledningen och konsistoriet.

I ansvaret ingår även att säkerställa att ledningssystemet, styrdokument, metodstöd och vägledningar är aktuella och ändamålsenliga, genomföra uppföljningar av informationssäkerheten och att stödja verksamheten inom KI i frågor om informationssäkerhet. Därutöver ingår omvärldsbevakning och kompetensutveckling.

2.2 Praktiskt informationssäkerhetsarbete vid KI - fyra enkla steg

Som myndighet måste KI säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat. Det gäller egentligen i alla situationer, t.ex. vid inköp och upphandling, utveckling, drift och förvaltning, forskningsprojekt

och vid etablerande av nya samverkansorgan. Praktiskt ska detta ska ske genom att:

1. Klassificera information och övriga informationstillgångar genom att bedöma hur viktiga och skyddsvärd dessa är för verksamheten, med avseende på konfidentialitet, riktighet och tillgänglighet.
2. Identifiera, analysera och värderar risker.
3. Identifiera, ställa krav på och införa ändamålsenliga säkerhetsåtgärder.
4. Löpande utvärdera införda säkerhetsåtgärder och göra anpassningar vid behov.

Informationssäkerhetsarbetet, analyser och införda säkerhetsåtgärder ska dokumenteras.

2.3 HR-frågor

Alla som är verksamma inom KI ska bidra till en säker informationshantering och följa KI:s regler för informationssäkerhet. För att lägga en bra grund för detta ska verksamhetsansvariga inom KI:

Säkerställa identiteten genom ID-kontroll och göra anpassade bakgrundskontroller vid rekrytering av egen och inhyrd personal baserat på vilken roll som är aktuell och vilken typ av information personalen kommer att ta del av

Med start vid rekrytering hålla egen och inhyrd personal informerad om de interna regler, arbetssätt och stöd som är aktuella och relevanta.

Vara medveten om risker för insiderhot.

Informera medarbetare och anknutna m.fl. om rutiner för incidenthantering.

Utvärdera att interna regler, arbetssätt och stöd fungerar på avsett sätt.

Säkerställa att egen och inhyrd personal har en lämplig kunskapsnivå inom informationssäkerhetsområdet beroende på roll och arbetsuppgifter.

Utveckla och upprätthålla kompetens hos egen personal avseende. informationssäkerhet genom utbildning, informationsinsatser och övning.

Vid avslutande av anställning, anknytning eller avtalsperiod se till att informationstillgångar återlämnas, liksom att berörda görs medvetna om fortsatt tystnadsplikt.

2.4 Hantering av tillgångar

Verksamhetsansvariga inom KI ansvarar för att informationstillgångar är identifierade och bedömda med avseende på risker och behov av säkerhetshöjande åtgärder kopplat till rättsliga krav, avtalskrav och olika former av informationshantering. Informationshantering av externa parter ska regleras i avtal.

Ambitionen bör vara att vidta en rimlig uppsättning säkerhetsåtgärder för att balansera risker mot eventuella verksamhetbegränsningar. Återkommande uppföljning ska genomföras för att få underlag till förbättringsåtgärder.

KI:s centralt framtagna och förvaltade lösningar för lagring, delning och behandling av information ska användas i första hand. Information ska enbart behandlas i system och tjänster som har en tillräcklig säkerhetsnivå för respektive informationsklass.

Stöd för att klassificera information finns i KI:s metodstöd. *(Se mall för informationsklassning och avsnittet om informationsklassning på Medarbetarportalen.)*

Stöd för att bedöma säkerhetsnivåerna i system och tjänster finns i KI:s metod för systemklassning. *(Se Metod för systemklassning och Vägledning för systemklassning på Medarbetarportalen.)*

2.5 Säkerhetsåtgärder

Informationssäkerhet uppnås genom att införa organisatoriska, personalrelaterade, fysiska och tekniska säkerhetsåtgärder.

Arbetet med att identifiera vilka säkerhetsåtgärder som är relevanta ska göras enligt de fyra stegen i avsnitt 2.2. Det vill säga utgå från verksamhetens behov, resultatet av informationsklassning och relevanta

riskbedömningar samt externa krav på informationsbehandlingen och dess skydd i exempelvis lagar, förordningar och avtal.

Stöd för att ta fram säkerhetsåtgärder finns i verktyget Kontrollkatalogen.

Informationssäkerhetsarbetet inom KI följer internationell standard ISO/IEC 27002:2023 för säkerhetsåtgärder.

2.6 Anskaffning, utveckling och underhåll av system

Genom att tillämpa en livscykelhantering för KI:s system kan man effektivt hantera och skydda information från skapande till arkivering och avveckling. Informationssäkerhet vid upphandling, inköp och löpande innebär följande:

Den information som hanteras under upphandlingsarbetet behandlas på ett säkert sätt både inom KI och hos eventuella leverantörer.

Den färdiga lösningen, varan eller tjänsten uppfyller de krav på informationssäkerhet som har identifierats som nödvändiga under hela avtalsperioden.

För att ställa rätt och relevanta säkerhetskrav ska därför identifiering, klassning och riskanalys genomföras, jämför med avsnitt 2.2.

Vid leverans måste säkerhetskraven kontrolleras, verifieras och godkännas innan användning av produkter eller tjänster.

Samma principer gäller vid utveckling av nya lösningar. KI måste säkerställa att utvecklare hanterar information utifrån aktuellt skyddsvärde och att den utvecklade produkten har rätt säkerhet för den information som ska behandlas.

Förvaltning och underhåll av inköpta/upphandlade och utvecklade lösningar ska beakta säkerheten löpande i förvaltningsarbetet och uppdatera klassningar, riskbedömningar och säkerhetsåtgärder vid behov. *(Se Vägledning för säker utveckling och Vägledning för säkerhetstester och granskningar.)*

2.7 Leverantörsrelationer

Verksamhetsansvariga ansvarar för att informationsbehandling av extern part följer KI:s regler och kravnivåer på informationssäkerheten och att detta regleras i avtal. *(Se avsnitt 2.2.)*

Informationssäkerhetsaspekterna ska beaktas i den löpande förvaltningen och styrningen av leverantörsrelationen.

Baserat på leverantörsrelationens art och hur känslig information som hanteras ska ändamålsenliga former för uppföljningar, revisioner, granskningar och/eller tester fastställas, regleras i avtal och genomföras under avtalstiden. *(Se Vägledning för säkerhetstester och granskningar.)*

2.8 Informationssäkerhetsincidenter

Det ska finnas en process för rapportering och hantering av informationssäkerhets- och personuppgiftsincidenter med målet att negativa konsekvenser snabbt avvärjs och i förekommande fall rapporteras till tillsynsmyndigheter inom föreskriven tid.

Statistik över inträffade händelser ska sammanställas för lärande och för att vidta åtgärder på lång sikt.

En informationssäkerhetsincident är en händelse som kan innebära negativ påverkan på KI:s verksamhet och kan exempelvis handla om förlust eller obehörig åtkomst till information, stöld av IT-utrustning eller datavirusutbrott. En incident där personuppgifter förekommer benämns personuppgiftsincident och kan vara särskilt allvarlig samt omfattas av rapporteringskrav till tillsynsmyndigheter.

2.9 Kontinuitetsarbete

Verksamhetsansvariga ska bedöma behovet av att vidta åtgärder för att säkerställa att eventuella avbrott i tillgången till information och systemstöd inte får allvarliga konsekvenser för verksamheten. I verksamheter där det bedöms nödvändigt ska aktuella reservrutiner och i förekommande fall återstartsrutiner finnas framtagna och vara kända av berörd personal.

En avvägd servicenivå på drift och förvaltning av IT-lösningar och tjänsteleveranser bör dimensioneras utifrån behoven i verksamheten redan från start.

2.10 Kontroll, verifiering och uppföljning

För att kunna bedriva säker och kontinuerlig verksamhet ska kontroller, verifiering och uppföljning av KI:s tekniska tillämpningar göras.

Det här gäller t.ex. innan man behandlar känslig information i nyutvecklade mobilapplikationer och inköpta system/lösningar men också löpande i förvaltning. Det kan också finnas behov av kontroll och verifiering av säkerhetsåtgärder vid användning av ny mer oprövad teknik eller andra informationsbehandlingar eller situationer med en bedömd relativt hög risk.

Kontroll, verifiering och uppföljning av säkerhetsåtgärder kan göras på olika sätt och med olika frekvenser beroende på hur verksamhetskritisk informationen är. *(Se Vägledning för säkerhetstester och granskningar.)*

2.11 Efterlevnad

För att säkerställa att KI, som myndighet, arbetar på ett lämpligt och effektivt sätt med informationssäkerhet och utifrån det arbetet inför relevanta åtgärder ska oberoende granskningar genomföras. De oberoende granskningarna får genomföras av internrevision eller annan extern part.