Anvisningar om informationssäkerhet för verksamma vid Karolinska Institutet

Dnr 1-143/2025

Gäller fr.o.m. 2025-06-05

Karolinska Institutet

Anvisningar om informationssäkerhet för verksamma vid Karolinska Institutet

Innehåll

Diarienummer	Dnr föreg. version:	Beslutsdatum:	Giltighetstid:
Dnr 1-143/2025	Dnr 1-393/2019	2025-06-05	Fr.o.m. 2025-06-05 och tills vidare

Beslut:
Universitetsdirektör

Dokumenttyp:
Anvisningar

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.

1. Inledning

Dessa anvisningar beskriver de grundläggande regler för informationssäkerhet som gäller för samtliga som är verksamma inom KI, dvs. medarbetare, anknutna och övriga som utför olika former av informationshantering på uppdrag av KI.

Anvisningarna anger vad vi måste förhålla oss till inom respektive område.

Syftet med anvisningarna är att skydda KI:s informationstillgångar och att göra det enkelt för alla att arbeta på ett säkert sätt.

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

2. Regler för säker informationshantering

2.1 Allmänna regler

- Skydda dina inloggningsuppgifter – dela dem aldrig med andra. Du är personligt ansvarig för de aktiviteter som utförs via ditt användarkonto.
- Alla enheter som används för informationshantering inom KI:s verksamhet ska hållas uppdaterade. Nya uppdateringar innehåller ofta säkerhetsuppdateringar som minskar risken för att du ska råka ut för olika typer av hot.
- Använd aldrig samma lösenord till KI:s tjänster som du använder till privata tjänster. Anledningen är att skydda KI:s information mot bristande säkerhet i olika externa tjänster vilket kan leda till att obehöriga får tillgång till lösenord till KI:s system.
- Lås eller logga ut från din dator när du lämnar den utan uppsikt. Fysisk tillgång till en olåst dator är ett av de enklaste sätten att komma åt KI:s information.
- Tänk även på risken att utsättas för så kallad manipulationsförsök, motsvarande engelskans Social Engineering, då du kan utsättas för försök till stöld av KI:s information eller utrustning.

- Öppna inte bilagor eller länkar i e-post om du är osäker på vad de innehåller eller vem avsändaren är.
- Information tillhörande KI får inte hanteras i privata molntjänster, dvs. sådana som inte är upphandlade, inköpta eller som tillhandahålls av KI, eller i privata lagringsmedia och enheter.
- Håll dig informerad om KI:s regler och information inom informationssäkerhet.
- Som verksam vid KI är du ansvarig för att personuppgifter hanteras i enlighet med kraven i GDPR och offentlighets- och sekretesslagen.
- Det är inte tillåtet att missbruka KI:s resurser genom uppenbar felanvändning, t.ex. genom att ladda ned stora filer, filmer, mjukvara eller använda tillgängliga resurser i privat eller kommersiellt syfte.
- Brott mot gällande säkerhetsregler kan medföra att man fråntas sina åtkomsträttigheter till KI:s system.
- Misstankar om brottslig verksamhet polisanmäls.

2.2 Känslig information

Vid hantering av information som vid klassning bedömts vara känslig och skyddsvärd, t.ex. känsliga personuppgifter, måste du bl.a. tänka på att:

- Du bara får ta del av den känsliga information du behöver för att kunna utföra ditt arbete.
- Hantera känslig information i pappersformat på ett säkert sätt avseende lagring och utskrift så att inga obehöriga kan ta del av materialet.
- Känslig information får inte skickas via e-post.
- Ta hänsyn till vilken miljö du befinner dig i när du hanterar och talar om känslig information då risk finns att obehöriga kan ta del av uppgifterna.
- Känslig information endast får lagras, behandlas och transporteras i IT-system och lösningar som har godkänts för ändamålet.
- Utöver ovanstående regler ska de grundläggande principerna för dataskydd beaktas vid hantering av personuppgifter. De grundläggande principerna samt ytterligare vägledningar och fördjupad information om hur hanteringen av personuppgifter ska ske vid KI finns på Medarbetarportalens sidor om GDPR.

2.3 IT-utrustning och lagringsmedia

Vid hantering av IT-utrustning och lagringsmedia gäller bl.a. följande:

- KI:s utrustning ska användas för verksamhetsrelaterade ändamål.
- Privata enheter får endast anslutas till KI:s gästnätverk alternativt eduroam.
- Känslig information, t.ex. känsliga och integritetskänsliga personuppgifter samt annan information som omfattas av sekretess enligt OSL, får inte hanteras på privata enheter.
- KI:s centrala lösningar för lagring och delning av information ska alltid användas i första hand. Endast i undantagsfall när det inte är möjligt kan information lagras på annat sätt, givet att kraven på informationssäkerhet uppfylls.
- I det fall lokal hårddisk eller bärbar lagringsmedia används ska dessa säkerhetskopieras. Huvudregeln är dock att spara informationen i KI:s centrala lagringslösningar
- Datorer och mobiltelefoner ska skyddas fysiskt och inte lämnas obevakade.
- Datorer, mobiltelefoner, surfplattor etc. ska alltid skyddas mot obehörig åtkomst genom lösenordsskydd, pinkod eller motsvarande. *(Se KI:s lösenordsregelverk på Medarbetarportalen).*

2.4 Mobila enheter

Information på mobila enheter ska skyddas så att den inte kommer i orätta händer, manipuleras eller förloras. Manipulation eller förlust av mobil enhet som används i arbetet och som har möjlighet att kopplas upp mot organisationens interna nät kan användas för vidare attacker in i organisationen. Tänk därför på att:

- Smarta telefoner och surfplattor som tillhandahålls av KI är arbetsredskap. KI äger utrustningen och ansvarar för att förvalta och hantera den information som finns på dem. Du som medarbetare ska vara medveten om att arbetsgivaren har rätt att ta del av all

information på enheten, t.ex. e-post, sms, foton och kalenderanteckningar.
- Eftersom offentlighetsprincipen gäller kan det vara möjligt för utomstående att begära ut informationen på din dator, telefon eller surfplatta.
- Smarta telefoner och surfplattor är i grunden att betrakta som osäkra lagringsplatser. Du får inte hantera konfidentiell information i sådana om inte särskild säkerhetslösning, godkänd av KI:s centrala IT-säkerhetsfunktion, används.
- Det finns ett stort utbud av applikationer att ladda ner till smarta telefoner och surfplattor. Många av dessa kan innehålla skadlig kod. I syfte att minska denna risk får du endast ladda ner applikationer från App Store eller Google Play.
- Pinkoder, fingeravtryck eller annan autentisering ska användas för smarta telefoner och surfplattor. Då pinkoder används får ej enkla pinkoder som 0000, 1234 etc. användas, och inte samma pinkod som används i andra sammanhang.
- Uppdateringar från leverantörer eller telefontillverkaren som aviseras på din mobila enhet ska installeras skyndsamt.
- De mobila enheterna ska ha funktion för spårning och fjärrensning.

2.5 Internetanvändning

Den internetuppkoppling som KI tillhandahåller ska användas som ett arbetsredskap. Privat användning får endast ske i begränsad omfattning och så länge det inte påverkar ditt arbete.

Det är inte tillåtet att:

- Besöka webbsidor som innehåller våld, rasism, pornografi, brottslig verksamhet eller andra sidor som av etiska skäl inte är lämpliga. Undantag från denna regel kan göras då arbetet/forskningen kräver det. Detta ska då godkännas av närmaste chef.
- Ladda ner filer eller program som inte är verksamhetsrelaterade (t.ex. musik eller filmer).

- Använda Internet på ett sådant sätt att KI:s varumärke riskerar att ta skada.
- Vid all Internetanvändning lämnar man digitala spår efter sig.

2.6 E-post

Användningen av e-post regleras i KI:s riktlinjer om e-post. Utöver riktlinjerna bör du även tänka på att:

- E-post är ett vanligt medel för att sprida skadlig kod och information som uppmanar mottagaren att ge ifrån sig inloggningsuppgifter. Var därför försiktig när du mottar e-post från okända avsändare eller e-post med suspekt innehåll. Om du är osäker, kontakta din närmaste chef eller försök att verifiera avsändaren innan du agerar.
- Känslig information, information som omfattas av sekretess, integritetskänslig information och känsliga personuppgifter ska som regel inte skickas med e-post. Föreligger en situation där man undantagsvis bedömer att detta kan ske måste en krypteringslösning användas som kan säkerställa att informationen inte kommer obehöriga till del.
- Rapportera e-postmeddelanden som innehåller skräppost eller nätfiske, så kallat Spam eller phishing – i första hand direkt via funktionen i Outlook. Du kan även rapportera händelsen som en informationssäkerhetsincident, för statistikens skull.
- Om du får e-post som innehåller hotfulla meddelanden bör du spara e-postmeddelandet, kontakta närmaste chef samt anmäla händelsen som en informationssäkerhetsincident.

KI kan stänga av enskildas e-postkonton vid misstanke om brott eller missbruk av interna säkerhetsregler.

Det är heller inte tillåtet att:

- Skicka eller spara stötande information så som våld, pornografi och diskriminerande ord och bilder.
- Skicka eller vidarebefordra skräppost/spam och kedjebrev.
- Öppna, skicka eller vidarebefordra programfiler som inte är verksamhetsrelaterade.

- Automatiskt vidarebefordra e-post till extern e-postadress.
- Uppge privat/extern e-postadress som kontaktinformation på KI:s offentliga webbsidor.

2.7 Sociala medier

Användandet av sociala medier ska främst ske utifrån verksamhetens syften, t.ex. för att snabbt nå ut till olika målgrupper och ska följa KI:s riktlinjer för sociala medier. Du bör även tänka på att:

- Privat användning av sociala medier på arbetstid endast är tillåten så länge det inte påverkar ditt arbete.
- KI:s e-postadress inte får användas för tjänster som används privat.
- Känslig information som berör ditt arbete aldrig får kommuniceras genom sociala medier.
- Publicering av personuppgifter på sociala medier ska göras i enlighet med kraven i GDPR och med hänsyn till eventuell sekretess.
- Lösenord som används för autentisering till sociala medier inte får vara desamma som lösenorden som används för KI:s system.
- I övrigt gäller samma regler som vid Internetanvändning och användning av e-post. För ytterligare information, se Riktlinjer för sociala medier på Medarbetarportalen.

2.8 Distansarbete

Vid arbete på distans ska du tänka på följande:

- Distansanslutning mot KI:s nätverk endast får ske genom godkända kommunikationslösningar för distansanslutning som KI-VPN eller VPN Light. Kontakta IT-support för mer information.
- Endast utrustning som uppfyller KI:s säkerhetskrav får kopplas upp mot KI:s interna nätverk.
- Känslig information hanteras och förvaras på ett säkert sätt enligt gällande säkerhetskrav.
- Känslig information alltid ska krypteras vid lagring på flyttbara lagringsmedier så som bärbara datorer, USB-minnen eller mobiltelefoner.

2.9 E-möten

Det är ofta både enkelt och lämpligt att ersätta fysiska möten med e-möten. Inte minst kan vi spara mycket tid. Vi behöver då tänka på informationssäkerheten genom att:

- avgöra vilka moment och vilken information som lämpar sig för e-möten,
- endast verktyg som KI har upphandlat ska användas för e-möten, såsom Teams och Zoom,
- följa reglerna för hantering av känslig information/känsliga personuppgifter,
- använda tekniska inställningar för att minska risken för obehörig åtkomst till e-möten. Detta är extra viktigt för e-möten som bedöms komma att innehålla känslig information,
- genomföra e-möten i lämpliga miljöer och lokaler och skydda din skärm från insyn.

2.10 Åtkomst och användaridentitet

Avseende åtkomst och användaridentitet ska du tänka på följande:

- Du som användare är ansvarig för hanteringen av information och de aktiviteter som sker under perioden då du är inloggad med din användaridentitet i ett system.
- Dina användaridentiteter, lösenord och passerkort är personliga och får aldrig lånas ut till någon annan. Att låna ut dessa uppgifter kan innebära att du behöver stå till svars för den aktiviteten som har utförts i ditt namn. Omvänt får du heller inte arbeta utifrån någon annan persons användaridentitet.
- Du omedelbart ska rapportera till IT-support om du misstänker att någon obehörig känner till ditt lösenord eller om du tappat bort ditt passerkort.

2.11 Loggning och loggranskning

Avseende loggning och loggranskning gäller följande:

- All internetanvändning loggas.

- För alla IT-system som innehåller känsliga uppgifter genomförs loggning av alla användaraktiviteter, dvs. allt vi gör i IT-systemet.
- Syftet med loggningen är att kunna säkerställa att endast behöriga personer har tagit del av relevant information samt för att kunna utreda eventuella incidenter eller misstankar om oegentligheter eller brott.
- Loggranskning genomförs regelbundet.

2.12 Incidentrapportering

Som verksam vid KI ska du känna till vad som klassas som incident samt var och hur dessa ska rapporteras. Som användare ska du hjälpa till genom att:

- Snarast möjligt rapportera incidenter som kan påverka KI:s verksamhet. För information om vart incidenter ska rapporteras se Medarbetarportalen ”Rapportera en händelse”.
- Skyndsamt rapportera incidenter som innefattar personuppgifter.
- Även rapportera misstankar om incidenter.

Exempel på informationssäkerhetsincidenter är:

- Felaktig, olovlig eller skadlig hantering av information som kan innebära negativ påverkan för KI.
- Information som kommit i orätta händer.
- Stöld av utrustning eller fysiska dokument innehållande känslig information.
- Dataintrång.
- Skadlig kod (t.ex. virus) eller skadlig programvara.

När en incident innefattar personuppgifter klassificeras händelsen som en personuppgiftsincident. Dessa är KI:s dataskyddsombud skyldig att enligt GDPR rapportera till tillsynsmyndigheten. *Se Medarbetarportalen ”Rapportera en händelse”*.