Handledning i informationssäkerhet vi Karolinska Institutet

Denna handledning beskriver de regler du som verksam vid KI ska känna till för att kunna bidra till att skydda KI:s information. Mer detaljerad information och anvisningar finns i ”Riktlinjer och regler för informationssäkerhet vid Karolinska Institutet”.

Hantering av känslig information

Vid hantering av känslig information måste du bl.a. tänka på att:

- Du bara får ta del av den känsliga information som du behöver för att kunna utföra ditt arbete
- Känslig information i pappersform ska låsas in när den inte används.
- Känslig information endast får skickas i krypterad form när den skickas via e-post
- Känslig information aldrig ska diskuteras på allmän plats eller då risk finns att obehöriga kan ta del av uppgifterna.
- Känslig information endast får hanteras i system som har godkänts för ändamålet i en systemklassning.

Hantering av personuppgifter

Hantering av personuppgifter ska ske i enlighet med vid var tid gällande lagstiftning för hantering av personuppgifter som GDPR och för forskningsverksamheter även etikprövningslagen (2003:460). Vid hantering av personuppgifter gäller bland annat följande:

- Det måste finnas en rättslig grund och ett tydligt ändamål för personuppgiftsbehandlingen som ska utföras.
- Alla personuppgiftsbehandlingar vid KI ska anmälas till KI:s register över personuppgiftsbehandlingar. Instruktioner för hur detta görs finns på KI GDPR.
- Personuppgifter får endast hanteras i system som har godkänts för ändamålet i en systemklassning.
- Personuppgifter som klassas som känsliga enligt GDPR eller kan anses vara integritetskänsliga av andra skäl ska dessutom hanteras i enlighet med reglerna för hantering av känslig information. 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 KI GDPR.

IT-utrustning och bärbar media

Vid hantering av IT-utrustning och bärbar media ska du tänka på att:

- KI:s utrustning ska användas för verksamhetsrelaterade ändamål.
- Privata datorer får kopplas upp mot KI:s nätverk endast under förutsättning att de har ett grundläggande säkerhetsskydd installerat. Detta inkluderar t.ex. uppdaterat antivirusprogram, brandvägg och åtkomstskydd med lösenord som uppfyller KI:s regelverk. Känslig information, t.ex. känsliga och integritetskänsliga personuppgifter samt annan information som omfattas av sekretess enligt Offentlighets – och sekretesslagen, får inte hanteras på privata enheter.
- Information på lokal hårddisk eller bärbar media alltid ska säkerhetskopieras. Där så är möjligt ska informationen sparas på angivna och KI-godkända ställen.
- Information i datorer, mobiltelefoner och på papper ska skyddas fysiskt, dvs. de får inte lämnas obevakade
- Bärbara datorer ska alltid skyddas mot obehörig åtkomst genom lösenordsskydd, och mobiltelefoner, surfplattor etc. genom pinkod eller motsvarande. Känslig information ska krypteras då den lagras på bärbar IT-media. För mer information, se KI:s regelverk för lösenord.

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 som språngbräda för vidare attacker in i organisationen. Tänk på att:

- Smarta telefoner och surfplattor som tillhandahålls av Karolinska Institutet är att betrakta som arbetsredskap. KI äger utrustningen och den information som finns på dem. Du som medarbetare ska vara medveten om att arbetsgivaren har rätt att ta del av t.ex. sms, foton och kalenderanteckningar.
- Eftersom offentlighetsprincipen gäller kan det vara möjligt för utomstående att begära ut informationen på din 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 informations- eller IT-säkerhetsfunktioner, 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 ned applikationer från App Store eller Google Play.
- Pinkoder, fingeravtryck eller annan autentisering ska användas för inloggning på smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till bankomatkort.
- Uppdateringar från Google eller telefontillverkaren och som aviseras på din mobila enhet ska installeras skyndsamt.
- De mobila enheterna ska ha funktion för spårning och fjärrensning.

Användning av Internet

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.
- Ladda ner filer eller program som inte är verksamhetsrelaterade (inkl. t.ex. musik eller filmer)
- Ansluta en dator till nätverket samtidigt som den är uppkopplad mot ett annat nätverk.

Användning av e-post

E-postsystemet är till för verksamhetsrelaterade uppgifter. Privat användning får endast ske i begränsad omfattning och så länge det inte påverkar ditt arbete. Tänk på att:

- Känslig information ska alltid krypteras då den skickas via e-post. Kontakta lokalt IT-stöd för hjälp.
- Verksammas e-postkonton kan stängas vid misstanke om brott eller missbruk.
- Din e-postadress bör enbart användas i verksamhetsrelaterade sammanhang.
- Det är 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 icke godkänd e-postadress.
    - Uppge privat/extern e-postadress som kontaktinformation på KI:s offentliga webbsidor.

Användning av sociala medier

Användandet av sociala medier inom KI ska främst ske utifrån verksamhetens syften, t.ex. för att snabbt nå ut till olika målgrupper.

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 privat login/kommunikation via sociala medier
- Känslig information aldrig får kommuniceras genom sociala medier.
- Lösenord som används för inloggning till sociala medier inte får vara desamma som lösenorden som används för KI:s system.

I övrigt gäller samma regler som vid användning av epost. För ytterligare information, se kommunikationsavdelningens riktlinjer för sociala medier.

Distansarbete

Vid arbete på distans ska du tänka på att:

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

Åtkomst och användaridentitet

Avseende åtkomst och användaridentitet ska du tänka på att:

- 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.

- Du omedelbart ska rapportera om du misstänker att någon obehörig känner till ditt lösenord eller om du tappat bort ditt passerkort.

Loggning och loggranskning

Avseende loggning och loggranskning gäller följande:

- All internetanvändning loggas
- För alla system som innehåller känsliga uppgifter genomförs loggning av alla användaraktiviteter, d.v.s. allt vi gör i systemet.
- Syftet med loggningen är att kunna säkerställa att endast behöriga personer har tagit del av en viss information.
- Loggranskning genomförs regelbundet.

Incidentrapportering

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 informationssäkerheten. För information om vart incidenter ska rapporteras se medarbetarportalen.
- Snarast möjligt rapportera incidenter som innefattar personuppgifter.
- Rapportera incidenterna till prefekten eller till av denne utsedd person.
- 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 personuppgift klassas händelsen som en personuppgiftsincident. Dessa ska enligt GDPR rapporteras.
Rapporteringar av informationssäkerhetsincidenter görs genom att maila KI:s IT-support. Mailadress: it-support@ki.se

Vi har alla ett ansvar!

För att upprätthålla en tillräcklig skyddsnivå för information och systemmiljö måste vi arbeta gemensamt och kontinuerligt. Uppsatta säkerhetsregler ska tillämpas och efterlevas av samtliga verksamma inom KI, det vill säga alla medarbetare, studenter, uppdragstagare /anknutna och konsulter i verksamheten.

Informationssäkerhet baseras huvudsakligen på sunt förnuft och gott omdöme, där din kunskap och ditt agerande är avgörande. Sammantaget är detta viktiga förutsättningar som bidrar till att upprätthålla förtroendet för vår verksamhet och säkerställa den information som vi hanterar.

Brott mot gällande säkerhetsregler kan medföra förlust av åtkomsträttighet till KI:s IT-system. Detta kan ske genom beslut av prefekten i samråd med säkerhetschef/IT-chef. Allvarligare fall av missbruk eller andra liknande regelbrott anmäls till säkerhetschefen för vidare handläggning. Misstankar om brottslig verksamhet polisanmäl