Riktlinjer, regler och anvisningar för informationssäkerhet vid Karolinska Institutet

Dnr 1–393/2019

(ersätter Dnr 1–516/2013)

Version 3.0

Gäller från och med 2019-04-23

Karolinska Institutet

Revisionshistorik

Versions-nummer	Datum	Ansvarig	Ändringar mot tidigare version
1.0	2013-04-01		
2.0	2013-10-01	Annika Sjöborg, säkerhetschef	Ändrad dokumentstruktur – uppdelad i tre delar, åtgärder för att förbättra läsbarheten - läsanvisning samt förtydliganden i vissa textavsnitt.
3.0	2019-04-23	Annika Sjöborg, säkerhetschef	Anpassning till nya legala krav. Införande av ny metod och modell för informationsklassning. Reviderad dokumentstruktur för att förbättra läsbarheten.

Karolinska Institutet

Beslut

2019-04-23

Dnr: 1–393/2019

Sid: 1/1

Ledningssystem för informationssäkerhet vid Karolinska Institutet – LIS

Karolinska Institutets (KI) uppdrag är att genom forskning och utbildning bidra till att förbättra människors hälsa. I detta arbete utgör information i olika former väsentliga förutsättningar och tillgångar. Alla verksamma inom KI ska därför arbeta aktivt, effektivt och kontinuerligt med informationssäkerhet, det vill säga hur olika typer av information hanteras i olika sammanhang.

Till stöd för ett systematiskt arbete med informationssäkerheten inom KI har utarbetats ett ledningssystem som bland annat består av riktlinjer, regler och anvisningar vilka härmed fastställs enligt dokumentet.

Beslut i detta ärende har fattats av undertecknad universitetsdirektör efter föredragning av KI:s säkerhetschef Annika Sjöborg.

Per Bengtsson

Annika Sjöborg

Innehåll

Termer och definitioner

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behörighet	Användares rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Data	Representation av fakta i form av tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Information	Innebörd i data, d.v.s. hur data tolkas av människor.
Skyddsvärd eller känslig information	Information som kräver ett särskilt skydd. Kan exempelvis vara information som omfattas av eller kan komma att omfattas av sekretess, känsliga personuppgifter, information som kräver hög konfidentialitet eller information som av andra skäl ej bör spridas till obehöriga.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Syftar till att säkerställa informationens: • Konfidentialitet - att information endast är åtkomlig för behöriga personer • Riktighet - att information är tillförlitlig, korrekt och komplett • Tillgänglighet - att information är tillgänglig utifrån verksamhetens behov
Informationstillgång	Information som är av värde för organisationen. Även informationsbärande resurser, t.ex. papper, mjukvara och olika typer av hårdvara, klassas som informationstillgångar.
IT-resurs	IT-baserad komponent som hanterar information, t.ex. system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara.
Verksamhetskritiska IT-system	IT-system avses de som klassas i de två högsta klasserna i någon av aspekterna konfidentialitet, riktighet och tillgänglighet.
GDPR	General Data Protection Regulation eller Dataskyddsförordningen på svenska.
Personuppgift	All slags information som direkt eller indirekt kan knytas till fysisk person som är i livet.
Sekretess	Information som omfattas av sekretess enligt offentlighets- och sekretesslagen och som därför inte ska lämnas ut och bli allmänt tillgänglig.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.
Informationsägare	Den som ansvarar för hela eller delar av informationsinnehållet i ett system.
Lagringsmedia	T.ex. USB-minnen, externa hårddiskar och minneskort.
Informationssäkerhetsincidenter	Med informationssäkerhetsincident avses en händelse som har eller skulle kunnat ha påverkat informationens konfidentialitet, riktighet eller tillgänglighet.
Personuppgiftsincidenter	En informationssäkerhetsincident beträffande personuppgiftsincidenter

Läsanvisningar

Kapitel	Primär målgrupp	Innehåll	Sidor
A	Alla verksamma vid KI	Regler och information för hur information och IT ska hanteras i olika situationer.	6–12
B	De som arbetar i den verksamhetsnära förvaltning	Regler och anvisningar för informationssäkerhet för t.ex. informationsägare, systemägare och förvaltningsledare.	13–32
C	De som arbetar inom IT-verksamheten och den IT nära förvaltning	Regler och anvisningar för hur informationssäkerhet ska hanteras inom KI:s IT-miljö.	33–50
D	De som arbetar med IT-, informations eller fysisk säkerhet på KI, samt de som har ansvar för myndighetskontakt vid incidenter	Regler och anvisningar som främst riktar sig till olika säkerhetsfunktioner vid KI.	51–55
Bilaga 1	De med ett utökat ansvar för informationssäkerheten vid KI. Dessa är bland annat KI:s universitetsdirektör, säkerhetschef, informationsägare, IT-direktör och systemägare.	Beskrivning av KI:s informationssäkerhetsorganisationen med tillhörande ansvarsbeskrivningar	56–60
Bilaga 2	De på KI som arbetar med HR- och personalfrågor samt chefer med personalansvar	Regler och anvisningar för informationshantering vid rekrytering, anställning och avslut av anställning	61-62

Riktlinjerna för informationssäkerhet beskriver *att* något ska göras, samt visar på KI:s viljeriktning för informationssäkerhetsarbetet. **Reglerna** för informationssäkerhet beskriver *vad* som ska göras. Till ett antal av de områden som beskrivs i reglerna finns det ytterligare en detaljeringsnivå som beskrivs i **anvisningar** som ger en mer detaljerad beskrivning av *hur* olika aktiviteter ska utföras.

Riktlinjer för informationssäkerhet vid Karolinska Institutet

På Karolinska Institutet (KI) hanteras information i form av forskningsidéer, forskningsdata, tentor och många andra typer av information som av olika skäl måste skyddas. Behovet av att skydda informationen, och regleringar om hur informationen får hanteras, grundar sig bland annat i legala krav som KI omfattas av, krav från samarbetspartners och inte minst KI:s egen verksamhet. Våra IT-system har i sig en god skyddsnivå, KI:s övergripande skyddsnivå är dock inte bättre än den svagaste länken. Det är därför en förutsättning att alla verksamma vid KI följer de regler som finns och arbetar tillsammans med att nå KI:s informationssäkerhetsmål.

I vårt arbete utgör information i olika former väsentliga förutsättningar och tillgångar. Alla verksamma inom KI ska arbeta aktivt, effektivt och kontinuerligt med informationssäkerhet. Detta innebär att hantera information på ett sådant sätt som hindrar att information läcker ut till obehöriga, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs.

Målet med KI:s informationssäkerhetsarbete är att säkerställa:

- Konfidentialitet - att information endast är åtkomlig för behöriga personer
- Riktighet - att information är tillförlitlig, korrekt och komplett
- Tillgänglighet - att information är tillgänglig utifrån verksamhetens behov

En annan viktig aspekt som ska beaktas vid hantering av KI:s information är spårbarhet, det vill säga att det går att säkerställa vem som haft åtkomst till och potentiellt ändrat information.

KI:s säkerhetslösningar och tillhörande rutiner och processer ska baseras på hur kritisk och skyddsvärd informationen i fråga är. Genom detta tillvägagångssätt uppnås en skyddsnivå för informationen som är anpassad till risken.

Allt detta är viktiga förutsättningar som bidrar till att säkerställa förtroendet för den verksamhet som bedrivs i KI:s regi samt en viktig del i det övergripande arbetet med riskhantering, intern styrning och kontroll.

Dessa riktlinjer med tillhörande regler och anvisningar omfattar hela KI:s verksamhet, alltså samtliga verksamma, det vill säga alla medarbetare, studenter, uppdragstagare/anknutna och konsulter i verksamheten, men också lokaler, utrustning, processer, IT-system och information.

Säkerhetsarbetet avser all typ av information, oberoende av om informationen är i digital form, på papper eller om den är muntlig.

Informationssäkerhet baseras huvudsakligen på sunt förnuft och gott omdöme, där varje individs kunskap och agerande är avgörande.

Kapitel A: Informationssäkerhet för alla verksamma vid KI

Detta kapitel vänder sig till samtliga verksamma vid Karolinska Institutet, det vill säga medarbetare, studenter, uppdragstagare/anknutna och konsulter.

A1. Introduktion till informationssäkerhet

KI:s informationssäkerhet är inte bättre än den svagaste länken och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. Tekniskt skydd är nödvändigt, men medarbetares kunskap och riskmedvetenhet är en minst lika viktig del av KI:s informationssäkerhetsarbete.

För att upprätthålla en tillräcklig skyddsnivå för information och systemmiljö samt för att efterleva lagar och förordningar måste vi arbeta gemensamt och kontinuerligt. Uppsatta säkerhetsregler ska tillämpas och efterlevas av samtliga verksamma inom KI, det vill säga medarbetare, studenter, uppdragstagare/anknutna och konsulter. Det är viktigt att alla som har åtkomst till KI:s IT-system beaktar informationssäkerhetsaspekterna och förstår sina personliga skyldigheter.

Informationssäkerhet baseras huvudsakligen på sunt förnuft och gott omdöme, där alla verksammas kunskap och agerande är avgörande. Sammantaget är detta viktiga förutsättningar som bidrar till att upprätthålla förtroendet för, och säkerställa den information som hanteras inom, KI:s verksamhet.

Målet med dessa regler är att införa en basnivå för informationssäkerhet vid hantering av information inom KI. Alla verksamma ska vara medvetna om vikten av sin egen insats för att upprätthålla lämpligt skydd och en etisk och korrekt hantering av verksamhetens information.

Som organisation utsätts KI kontinuerligt för olika säkerhetsrisker, exempelvis brand, stöld och oavsiktlig eller avsiktlig skadegörelse, obehörig åtkomst till information och olaglig hantering av data. Om dessa risker förverkligas kan det leda till problem såsom brutet förtroende och kränkt integritet, ekonomisk skada eller andra former av förluster, samt att KI:s anseende skadas. Dessutom kan det leda till skada för enskild individ eller annan parts verksamhet.

Informationssäkerhet handlar om att skydda informationens konfidentialitet, riktighet och tillgänglighet, oberoende av om informationen är i digital form, på papper eller om den är muntlig.

- Konfidentialitet - att information endast är åtkomlig för behöriga personer. Exempelvis att tentor, forskningsresultat och forskningsdata inte är åtkomlig för obehöriga innan publicering.
- Riktighet - att information är tillförlitlig, korrekt och komplett. Exempelvis att forskningsdata och betygsunderlag inte förvanskas och i förlängningen leder till felaktiga beslut.
- Tillgänglighet - att information är tillgänglig utifrån verksamhetens behov. Exempelvis att vi har tillgång till den informationen och de IT-system som krävs för att vi ska kunna utföra vårt arbete.

Reglerna och tillhörande anvisningar bildar tillsammans ett ramverk för KI:s skydd av informationstillgångar inom organisationen. För att lyckas med dessa informationssäkerhetsinsatser är det nödvändigt att alla verksamma förstår sitt ansvar och med-verkar för att efterleva regelverket. Dokumentet utgör KI:s övergripande regelverk för hantering av verksamhetens information. Reglerna baseras på gällande lagar och föreskrifter, däribland Myndigheten för samhällsskydd och beredskap, MSB:s, föreskrift om statliga myndigheters

informationssäkerhet (MSBFS 2016:1)[1] samt ISO-standarden för informationssäkerhet (SS-ISO/IEC 27001:2013).

A2. Handledning för informationssäkerhet

Samtliga verksamma, det vill säga medarbetare, studenter, uppdragstagare/anknutna och konsulter, ansvarar för att känna till och följa gällande regler för informationssäkerhet inom Karolinska Institutet. I denna handledning beskrivs de regler som alla verksamma vid KI ska känna till för att kunna bidra till att skydda verksamhetens känsliga information.

Informationssäkerhet – 9 saker att tänka på

1. Skydda dina inloggningsuppgifter och lämna aldrig ut dem. Du är personligt ansvarig för de aktiviteter som utförs via dina inloggningsuppgifter.
2. Håll dina enheter uppdaterade. Nya uppdateringar innehåller ofta säkerhetsuppdateringar som minskar risken för att du ska råka ut för olika typer av hot.
3. Använd aldrig samma lösenord till KI:s tjänster som du använder till privata tjänster. KI kan inte granska säkerheten i tjänster som används privat och bristande säkerhet i sådana tjänster kan leda till att obehöriga får tillgång till lösenord till KI:s system.
4. Lås eller logga ut från din dator när du går därifrån. Fysisk tillgång till en olåst dator är ett av de enklaste sätten att komma åt KI:s information.
5. Undvik att skicka känslig information via e-post. Om så sker ska den krypteras. Kontakta IT-support för hjälp.
6. Ladda inte ner filer från internet och öppna inte bilagor eller länkar i e-post om du är osäker på vad de innehåller eller vem avsändaren är.
7. Tänk på i vilken miljö du befinner dig när du hanterar och talar om känslig information.
8. Se till att din information är säkerhetskopierad oavsett om den är lagrad på stationär dator, bärbar dator eller bärbart IT-media. Kontakta IT-support för hjälp.
9. Information tillhörande KI får inte hanteras i privata molntjänster (sådant som inte är upphandlade, inköpa eller som tillhandahålls av KI) eller i privata lagringsmedia eller enheter.
10. Som verksam vid KI är du ansvarig för att personuppgifter hanteras i enlighet med kraven i GDPR.

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 du behöver för att kunna utföra ditt arbete.
- Känslig information i pappersform ska låsas in när den inte används.
- Känslig information endast får skickas krypterat 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.

[1] MSB:s föreskrift om statliga myndigheters informationssäkerhet, https://www.msb.se/externdata/rs/b74a7b16-36a5-4de8-8f15-1297c37f1324.pdf

- Känslig information endast får hanteras i IT-system som har godkänts för ändamålet efter genomförd systemklassning, se *kapitel B2, Informations- och 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:s GDPR-sida[2].
- Personuppgifter får endast hanteras i IT-system som har godkänts för ändamålet efter genomförd systemklassning, se *avsnitt B2, Informations- och 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[3].

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:s GDPR-sida[2].

IT-utrustning och lagringsmedia

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

- KI:s utrustning ska användas för verksamhetsrelaterade ändamål.
- Privata datorer får endast kopplas upp mot 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.
- Information på lokal hårddisk eller bärbar lagringsmedia ska alltid 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 dator och/eller lagringsmedia. För mer information, se KI:s regelverk för lösenord[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

---

[2] KI:s GDPR-sida, https://ki.se/medarbetare/gdpr-pa-karolinska-institutet

[3] KI:s GDPR-sida om känsliga personuppgifter https://ki.se/medarbetare/kansliga-personuppgiftersarskilda-kategorier-av-personuppgifter

[4] KI:s regelverk för lösenord, https://ki.se/medarbetare/regler-for-losenord-pa-karolinska-institutet

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 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, t.ex. pinkod till bankomatkort.
- Uppdateringar från leverantörer 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[5].
- Ladda ner filer eller program som inte är verksamhetsrelaterade (inkl. t.ex. musik eller filmer).

Användning av E-post

Användningen av e-post regleras i KI:s regler och riktlinjer för användning av e-post[6]. Utöver dessa regler och riktlinjer 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.

---

[5] Undantag från denna regel kan göras då arbetet/forskningen kräver det. Dessa undantag ska godkännas av närmaste chef.

[6] KI:s regler och riktlinjer för användningen av e-post. https://ki.se/medarbetare/regler-och-riktlinjer-for-anvandning-av-e-post

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 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.
- 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 användning av e-post. För ytterligare information, se kommunikationsavdelningens riktlinjer för sociala medier[7].

Distansarbete

Vid arbete på distans ska du tänka på att:

- Distansanslutning mot KI:s nätverk endast får ske genom godkända kommunikationslösningar för distansanslutning. Kontakta IT-support för mer information.
- 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 lagringsmedier 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 till IT-support 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.

---

[7] KI:s riktlinjer för sociala medier, https://ki.se/medarbetare/sociala-medier?_ga=2.150283382.1128184671.1538394890-677769654.1536223025

- För alla IT-system som innehåller känsliga uppgifter genomförs loggning av alla användaraktiviteter, d.v.s. 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.

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[8].
- Skyndsamt 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 personuppgifter klassas händelsen som en personuppgiftsincident. Dessa är KI:s dataskyddsombud skyldig enligt GDPR att rapportera till tillsynsmyndigheten. För den senaste informationen om hur personuppgiftsincidenter ska hanteras se medarbetarportalen[8].

A3. Efterlevnad

Kontinuerlig kontroll av efterlevnaden av gällande informationssäkerhetskrav är en förutsättning för att upprätthålla en god informationssäkerhet inom Karolinska Institutet. Att förstå vikten av och efterleva dessa krav är helt avgörande för hanteringen av KI:s information och i slutändan förtroendet för KI:s verksamhet.

En god förståelse av angivna krav och villkor för hela KI:s informationssäkerhet krävs av samtliga verksamma för att hantera informationssäkerheten på ett bra och effektivt sätt. Säkerhetskrav och skydd behöver kontinuerligt utvärderas för att säkerställa att skyddsnivån över tiden är rätt i relation till identifierade risker. Vidare är det viktigt att säkerställa att fastställda säkerhetsregler efterlevs och uppfylls.

Brott mot gällande säkerhetsregler kan medföra att verksamma fråntas sina åtkomsträttigheter till KI:s system. Beslut om detta fattas av säkerhetschefen i samråd med universitetsdirektör eller IT-säkerhetsansvarig. IT-säkerhetsansvarig på KI har även rätt att temporärt frånta rättigheter vid upptäckt av brott mot regelverket innan ett formellt beslut har fattats.
Allvarligare fall av missbruk, eller andra liknande regelbrott, ska anmälas till säkerhetschefen för vidare handläggning. Misstankar om brottslig verksamhet ska polisanmälas.

[8] KI:s informationssäkerhetssida på Medarbetarportalen, https://ki.se/medarbetare/informationssakerhet

Kapitel B: Informationssäkerhet för den verksamhetsnära förvaltning

Kapitel B innehåller regler och anvisningar som specifikt rör den verksamhetsnära förvaltning, främst avsett för systemägare, informationsägare och förvaltningsledare. För ansvarsbeskrivningar för dessa roller se Bilaga 1, Informationssäkerhetsorganisation och ansvarsbeskrivningar.

B1. Hantering av tillgångar

På Karolinska Institutet finns tillgångar som är nödvändiga för den verksamhet som bedrivs, t.ex. informationstillgångar i form av forsknings- och utbildningsdata. Dessa tillgångar måste hanteras på sådant sätt att det går att säkerställa att de skyddas mot obehörig åtkomst, felaktiga förändringar och att de finns tillgängliga då de behövs.

Grundläggande säkerhet

För alla informationstillgångar inom KI ska det finnas utsedda informations- och systemägare. Det ska finnas en förteckning över informationstillgångarna och vilka som är ansvariga för dessa. Dessutom ska alla informationstillgångar inom KI klassas utifrån informationstyp för att klargöra hur betydande tillgången är för verksamheten och vilka krav på säkerhetsåtgärder och hantering som gäller, *se kapitel B2, Informations- och systemklassning* för mer information.

Hanteringskrav för vissa typer av information

Personuppgifter	Hantering av personuppgifter ska ske i enlighet med GDPR.
Skyddade personuppgifter	Skyddade personuppgifter ska hanteras enligt kapitel 22 i Offentlighets- och sekretesslagen (2009:400).
Utlämnande av information	Det ska finnas instruktioner för utlämnande av information där det framgår vem eller vilka som har rätt att fatta beslut kring utlämnande. Före utlämnande ska en sekretessprövning alltid göras. Se KI:s riktlinjer om allmänna handlingar och utlämnande[9].
Extern informations-hantering	Då KI:s information hanteras av tredje part, till exempel externa leverantörer, ska kraven avseende informationssäkerhet specificeras i avtal mellan leverantören och KI. Om informationen innefattar personuppgifter ska ett personuppgiftsbiträdesavtal upprättas.
Extern åtkomst till information	Vid tillgång till KI:s information från miljöer utanför KI:s kontroll ska specifika krav ställas på autentisering och kryptering.
Överföring av personuppgifter utanför EU och EES	För överföring av personuppgifter till länder utanför EU och EES gäller särskilda regler. Kontakta alltid KI:s dataskyddsombud innan överföring görs.

Anvisning för hantering av personuppgifter

Hantering av personuppgifter inom Karolinska Institutet regleras av GDPR och för forskningsverksamheter även etikprövningslagen (2003:460). Personuppgifter ska alltid hanteras i enlighet med vid var tid gällande lagstiftning och denna anvisning utgör ett stöd för att definiera den miniminivå på skyddsåtgärder för personuppgifter som ska följas inom KI.

Känsliga personuppgifter

Behandling av känsliga personuppgifter kräver att särskilda skyddsåtgärder har vidtagits. Val av skyddsåtgärder bör göras i samråd med KI:s dataskyddsombud, IT-säkerhetsansvarig och/eller informationssäkerhetsfunktion.

[9] KI:s riktlinjer om allmänna handlingar och utlämnande, https://ki.se/medarbetare/allmanna-handlingar-och-utlamnande

Utlämnande av personuppgifter

För att hantera de registrerades, myndigheters och andra aktörers begäran om information ska det finnas instruktioner för hantering vid utlämnande av personuppgifter. Av instruktionerna ska det framgå vem eller vilka som har rätt att fatta beslut om utlämnande. Innan utlämnande görs ska alltid en sekretessprövning om utlämnade i enlighet med Offentlighets- och sekretesslagen (2009:400) kan genomföras.

Personen som lämnar ut information ska alltid försäkra sig om att det är rätt person som tar emot informationen.

För ytterligare information, se KI:s anvisningar om utlämnande av allmänna handlingar[10].

Lagring av personuppgifter

Lagring av personuppgifter får bara ske i system och/eller applikationer som efter genomförd informationsklassning är godkända för personuppgiftslagring.

Känsliga personuppgifter som lagras i bärbara datorer och på löstagbara lagringsmedier ska vara krypterade, och hanteras på ett sådant sätt att obehöriga inte kan ta del av uppgifterna. Kontakta IT-support för med information.

Bevarande, rensning och gallring av personuppgifter

Personuppgifter ska bevaras, rensas och gallras enligt aktuell lagstiftning och det ska finnas dokumenterade instruktioner avseende hur detta ska hanteras inom KI.

B2. Informations- och systemklassning

Vissa informationstillgångar är mer känsliga, värdefulla eller kritiska än andra. Behovet av skydd skiljer sig därför mellan olika typer av informationstillgångar. Informations- och systemklassning är grundläggande komponenter i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för, och kan styra vilket skydd som krävs för olika typer av information. IT-system som hanterar KI:s information ska ha en klassningsprofil som baseras på den information IT-systemen hanterar eller ska kunna hantera. Systemklassningen styr vilka säkerhetsåtgärder som ska tillämpas för det enskilda IT-systemet. Informationsklassning är ett krav i MSBFS 2016:1 samt i ISO 27001.

Grundläggande säkerhet

Information inom KI ska ha utsedda informationsägare som bl.a. ansvarar för att den hanteras och skyddas utifrån hur känslig och värdefull den är. En etablerad metod för att värdera information är genom s.k. informationsklassning. Detta görs genom att bedöma vilken konsekvens bristande konfidentialitet, riktighet respektive tillgänglighet av informationen riskerar medföra.

- **Konfidentialitet** – att information inte tillgängliggörs eller avslöjas för obehöriga.
- **Riktighet** – att information är tillförlitlig, korrekt och komplett.
- **Tillgänglighet** – att informationen är tillgänglig utifrån verksamhetens behov.

[10] KI:s anvisningar om allmänna handlingar och utlämnande https://ki.se/medarbetare/allmanna-handlingar-och-utlamnande

Informationsklassningen skapar kunskap, medvetenhet och samsyn om hur känsliga, värdefulla eller kritiska informationstillgångar av olika slag är. Genom att ha en riskbaserad säkerhet, kan vi förebygga kostsamma incidenter, men också en onödigt hög säkerhetsnivå, vilket kommer resultera i högre kostnader och skapa en onödigt krånglig informationshantering.

Klassningen ska ta hänsyn till rättsliga krav som lagar och föreskrifter, men även interna krav eller bedömningar av informationens värde, känslighet och betydelse.

Informationsklassningen leder till konkreta krav på säkerhetsåtgärder i IT-system (såväl interna som externa) och ska omprövas regelbundet som en del i KI:s systematiska säkerhetsarbete.

Anvisning för informationsklassning

Informationsägare vid KI ansvarar för att klassning görs för information som de äger. Klassningen ska genomföras utifrån de tre säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Varje aspekt har fyra konsekvensnivåer (0–3). Konsekvensnivåerna i klassningsmodellen har samma nivåer som i KI:s modell för riskanalys, se figur 1. Dessa är *Allvarlig, Kännbar, Lindrig* och *Försumbar*. För mer detaljerad information av respektive värderingsnivå, se KI:s kriterier för riskvärdering[11].

Säkerhets-aspekt / **Konsekvensnivå**	**Konfidentialitet (K)**	**Riktighet (R)**	**Tillgänglighet (T)**
3	**Allvarlig** negativ påverkan för KI, enskild individ eller tredje part vid bristande konfidentialitet, riktighet eller tillgänglighet.		
2	**Kännbar** negativ påverkan för KI, enskild individ eller tredje part vid bristande konfidentialitet, riktighet eller tillgänglighet.		
1	**Lindrig** negativ påverkan för KI, enskild individ eller tredje part vid bristande konfidentialitet, riktighet eller tillgänglighet.		
0	**Försumbar** negativ påverkan, enskild individ eller tredje part vid bristande konfidentialitet, riktighet eller tillgänglighet.		

Figur 1. KI:s informationsklassningsmodell

Några grundläggande frågor man ska ställa sig när man klassar information är:

- Vilka blir konsekvenserna för KI, enskild eller tredje part om informationen läcker till obehöriga (konfidentialitet)?
- Vilka blir konsekvenserna för KI, enskild eller tredje part om informationen är felaktig eller inaktuell (riktighet)?
- Vilka blir konsekvenserna för KI, enskild eller tredje part om behöriga inte har tillgång till informationen (tillgänglighet)?

Som stöd vid informationsklassning finns ett internt underlag med fördefinierade klassnings-profiler för olika kategorier av information. Detta kommer successivt fyllas på vartefter information inom KI identifieras och klassas. Det är dock viktigt att varje informationsägare tar ställning till om den fördefinierade klassningen är tillämplig även för sin information. Underlaget

[11] KI:s sida om Intern styrning och kontroll på Medarbetarportalen https://ki.se/medarbetare/intern-styrning-och-kontroll

finns på KI:s informationssäkerhetssida på medarbetarportalen[12]. Där hittar man även övriga processbeskrivningar, mallar och instruktioner för klassningsarbetet.

Informationsklassningen utgör dels underlag vid systemklassning och med det krav på säkerhetsåtgärder i IT-system och dels underlag för hanteringskrav då information hanteras utanför system.

Anvisning för systemklassning

En viktig uppgift för systemägare är att klassa sina system, s.k. *systemklassning*. Alla system, interna och externa, som hanterar KI:s information ska klassas. Systemklassningen ska baseras på klassningen av den information som IT-systemet hanterar. Ett systems klassningsprofil baseras på den högst klassade ingående information som IT-systemet hanterar för respektive säkerhetsaspekt. Se figur 2 nedan.

Informationskategori	Konfidentialitet	Riktighet	Tillgänglighet
Informationstyp 1	3	1	1
Informationstyp 2	0	1	1
Informationstyp 3	2	2	2
IT-systemets klassningsprofil	**3**	**2**	**2**

Figur 2. Exempel på systemklassning

Det viktigaste vid systemklassning är att den mest känsliga informationen, dvs. informationen med högst skyddskrav i någon av de tre informationssäkerhetsaspekterna, är identifierad och klassad så att tillräckligt skydd för informationen kan skapas för IT-systemet.

Systemklassningen utgör underlag för kravställning på säkerhetsåtgärder, hämtade från standarden ISO 27001. Detta gäller oavsett om IT-systemet är internt eller externt (outsourcing eller molntjänst). Mottagare av kravställningen är normalt interna förvaltningsorganisationer respektive externa leverantörer.

En initial klassning ska alltid göras vid upphandling eller utveckling av IT-system i syfte att i ett tidigt skede i processen kunna säkerställa IT-systemets säkerhetsnivåer.

B3. Riskhantering

Den information och de IT-system som används inom KI är viktiga för att bedriva verksamheten och måste skyddas på lämpligt sätt. För att avgöra hur KI ska skydda information och IT-system på rätt sätt måste relaterade risker identifieras och analyseras. Riskanalyser ska vara en naturlig del av KI:s arbetssätt och bidra till att verksamheten kan bedrivas på ett ändamålsenligt och effektivt sätt.

Grundläggande säkerhet

För att säkerställa att information hanteras på ett säkert sätt ska hot och risker relaterade till information kontinuerligt identifieras, analyseras och hanteras med lämpliga skyddsåtgärder. För att komma fram till vilka skyddsåtgärder som är lämpliga för respektive informationstillgång ska riskanalyser genomföras kontinuerligt.

[12] KI:s informationssäkerhetssida på Medarbetarportalen, https://ki.se/medarbetare/informationssakerhet

Riskanalyser gör det möjligt för informations- och systemägare att identifiera huvudsakliga risker. Dessa bedöms sedan utifrån hur stor sannolikheten är att hoten realiseras samt potentiella konsekvenser. Analysen ger underlag för att avgöra vilka skyddsåtgärder som krävs för att säkerställa att riskerna, dvs. konsekvensen och sannolikheten för att ett hot inträffar, hanteras och minimeras på lämpligt sätt. Alla skyddsåtgärder ska dokumenteras på ett sådant sätt att det är möjligt att kontrollera efterlevnaden.

Inom KI ska riskanalyser vara en naturlig del av hanteringen av information och genomföras på flera olika nivåer; på övergripande organisationsnivå, på institutionsnivå, avseende specifika IT-system eller informationstillgångar etc. Riskanalyser för informationssäkerhet ska utgå från aspekterna konfidentialitet, riktighet och tillgänglighet för den analyserade informationen. Riskanalyser ska genomföras i samband med förändringar i verksamheten, processerna och systemen. För alla verksamhetskritiska IT-system ska riskanalyser genomföras årligen. I samband med detta ska det även analyseras om det finns nya, eller förändrade, interna eller externa krav som påverkar det aktuella IT-systemet. Till alla identifierade risker ska det utses en ansvarig som svarar för att säkerställa att de hanteras på ett lämpligt sätt. Uppföljning ska ske av att identifierade risker åtgärdas, alternativt hanteras på annat sätt, inom en rimlig tid.

Resultatet från genomförda riskanalyser ska rapporteras till säkerhetschefen via informationssäkerhetssamordnaren.

Anvisning för genomförande av riskanalyser

I enlighet med *Regler och riktlinjer för intern styrning och kontroll* vid KI, Dnr 1795/2009–010, ska riskanalyser genomföras regelbundet på olika nivåer och olika områden inom KI:s verksamhet. Det finns olika metoder och modeller för att genomföra riskanalyser. Inom KI finns en beslutad riskanalysmetod som företrädesvis ska användas. Oavsett vilken metod som används ska nedanstående aktiviteter alltid utföras vid genomförandet av en riskanalys.

1. **Analysens omfattning och avgränsning ska definieras**
   Ramarna för den riskanalys som ska genomföras sätts genom att det område eller den process som ska analyseras definieras och avgränsas. Riskanalysmetod ska väljas och personer med god kännedom om aktuellt område/process ska identifieras och bjudas in att delta i analysen. Dessa personer ska också ges tillfälle att förbereda sig och inhämta nödvändig information/fakta för att kunna genomföra uppgiften på ett effektivt och ändamålsenligt sätt.
2. **Hot ska identifieras**
   För varje delområde, eller steg i processen, som analyseras ska de hot som föreligger identifieras, grupperas och dokumenteras. Hoten ska dokumenteras på tillräcklig detaljnivå så att även utomstående förstår vad som avses.
3. **Konsekvens och sannolikhet ska bedömas**
   Vilka konsekvenserna blir om identifierade hot inträffar, och hur sannolikt det är att de inträffar, ska identifieras, analyseras och resultatet dokumenteras. Omfattningen av risken, dvs. konsekvensen och sannolikheten för att ett hot inträffar, bör bedömas utifrån en definierad metod som också gör det möjligt att jämföra risker och deras omfattning.
4. **Åtgärdsförslag ska utarbetas**
   Det kan ligga flera olika orsaker bakom varje identifierad risk, och förslag för att hantera dessa måste därför arbetas fram. Konsekvensen av förslagen måste analyseras innan beslut om hur risken hanteras fattas. Att hantera en risk kan exempelvis vara att vidta åtgärder

för att förhindra eller minska sannolikheten för att de bakomliggande orsakerna inträffar, eller att konsekvenserna av om de inträffar minimeras.

5. **Riskanalysen ska dokumenteras**
   En rapport ska sammanställas utifrån den genomförda riskanalysen. Rapporten bör, förutom själva analysresultatet och beskrivningen av de risker man funnit, innehålla information kring alla steg i genomförandet av riskanalysen. Rapporten bör även innehålla eventuella förslag till hur riskerna ska hanteras och rekommendationer till den som ska fatta beslut i frågan. Dessa förslag ska ligga till grund för planering av det fortsatta arbetet kring riskhanteringen.
6. **Handlingsplan ska tas fram och följas upp**
   En prioriterad handlingsplan, med angivande av vilka åtgärder som ska vidtas, vem som ansvarar för dessa och när de ska vara genomförda ska tas fram och följas upp. Föreligger det risker för vilka verksamheten bedömer att det inte behövs några åtgärder ska även denna accept av kvarvarande risker dokumenteras.

B4. Styrning av kommunikation och drift

Inom Karolinska Institutets verksamhet finns beroenden till olika IT-system och den information som hanteras där. Det är av stor vikt att dessa IT-system vid behov finns tillgängliga för att verksamheten ska kunna bedrivas effektivt. Den information som kommuniceras och överförs i KI:s nätverk ska skyddas så att inte obehöriga kan ta del av den.

Grundläggande säkerhet

Kommunikation

När information överförs genom data- eller telekommunikation uppstår risk för obehörig åtkomst och förändring av den överförda informationen. Respektive informationsägare svarar för att analysera behovet av nödvändiga skyddsåtgärder, relaterat till riskerna för obehörig åtkomst eller förändring, samt att dessa dokumenteras på lämpligt sätt. Informationsägare ska kommunicera sina behov till KI:s IT-direktör, som ansvarar för kravställningen avseende nätverket.

Drift

Systemägaren till en specifik IT-resurs (system/applikation, nätverk, teknisk plattform etc.) ansvarar för kravställning avseende dess driftsäkerhet. Kravställningen baseras normalt på informations- och systemklassning samt riskanalys.

Anvisning för kravställning av driftsäkerhet och servicenivå

Anvisningen anger den miniminivå som ska följas inom Karolinska Institutet och utgör även ett stöd för att definiera vilka områden som exempelvis, men inte uteslutande, bör ingå i kravställningen.

Känslig information får aldrig överföras på ett sådant sätt att obehöriga kan ta del av informationen. Detta innebär att överföring via öppna nät i regel måste vara krypterad.

All IT-utrustning som kopplas till KI:s nät ska vara konfigurerad enligt definierad standard och det ska finnas instruktioner för hantering av sådan utrustning. Övriga datorer som behöver kopplas upp mot internet ska separeras från KI:s interna nätverk och anslutas via ett så kallat gästnät.

Systemägaren till en specifik IT-resurs (system/applikation, nätverk, teknisk plattform etc.) ansvarar för att i samråd med informationssäkerhetsfunktionen och/eller IT-säkerhetsansvarig kravställa IT-resursen avseende dess driftsäkerhet, vilken omfattas av följande områden:

säkerhetsuppdateringar, förändringshantering, kapacitetsplanering, skydd mot skadlig kod, säkerhetskopiering, återläsning av data samt system- och driftsdokumentation. Kravställningen baseras normalt på informations- och systemklassning samt riskanalys.

Då KI köper tjänster eller förlägger drift av IT-resurser utanför den egna organisationen ska samma regler avseende informationssäkerhet gälla som när driften hanteras i egen regi. Kraven på informationssäkerhet ska definieras baserat på en dokumenterad informationsklassning och riskanalys och kraven ska regleras i avtal parterna emellan. Ägaren till den specifika IT-resursen ansvarar för kravställning och uppföljning av dessa krav, men samordning bör ske i de fall leverantören hanterar flera av KI:s IT-resurser.

Om tjänsten eller driften av IT-resursen innefattar behandling av personuppgifter ska även ett personuppgiftsbiträdesavtal i enlighet med GDPR upprättas mellan parterna.

Separerade miljöer

Produktions-, utvecklings-, test-, och utbildningsmiljöer ska vara separerade. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för utvecklings- och testmiljöerna.

Drift och driftsdokumentation

Drift av KI:s IT-resurser ska ske i enlighet med god praxis och dokumenterade, implementerade processer. Det ska finnas dokumenterade och kontinuerligt uppdaterade operationella driftsrutiner och driftsinstruktioner, och all drift ska ske i enlighet med dessa. Den dokumenterade driftsdokumentationen ska uppdateras vid behov och revideras minst årligen eller när behov i övrigt föreligger. Där så är möjligt ska bevis på att rutinerna/instruktionerna följs dokumenteras och lagras. Kopior av driftsdokumentationen ska förvaras separerade från originalen och arkivering av dokumentationen ska ske i enlighet med fastställda rutiner.

Säkerhetsuppdateringar

Säkerhetsuppdateringar avseende operativsystem och program ska hanteras kontrollerat och skyndsamt. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön. Om analysen påvisar att säkerhetsuppdateringen genererar risker för stabiliteten i produktionsmiljön ska en dokumenterad motivering finnas för varför säkerhetsuppdateringen inte genomförs.

Detaljerade anvisningar ska finnas för hantering av akuta säkerhetsuppdateringar, det vill säga säkerhetsuppdateringar som måste installeras så skyndsamt att de inte hinner testas. Instruktionerna bör säkerställa att tester genomförs efter installationen, och att åtgärder vidtas baserat på testernas resultat.

Förändringshantering

Alla förändringar som görs i KI:s IT-system ska noggrant planeras och analyseras, och alla förändringar, liksom test och överföring till produktionsmiljön av dessa, ska vara formellt godkända av behörig person. Godkännanden ska dokumenteras och lagras.
Dualitetsprincipen bör tillämpas – det vill säga utveckling, test och produktionssättning bör inte ske av en och samma person och ska ske i separata miljöer. Utvecklings- och testmiljön får inte, utan att särskilda, av systemägaren godkända, säkerhetsåtgärder vidtagits, innehålla känslig information.

Det ska finnas detaljerade anvisningar för hur förändringar ska hanteras och testas, liksom planer för att, vid behov, kunna återgå till läget innan förändringen påbörjades.

Detaljerade anvisningar ska även finnas för akuta förändringar som måste åtgärdas omgående, och där tid inte finns för att följa den normala förändringsprocessen. Sådana förändringar kan exempelvis vara störningar i produktionsmiljön. Akuta förändringar ska dokumenteras och i efterhand följas upp enligt detaljerade anvisningar för akut förändringshantering.

Kapacitetsplanering

Syftet med kapacitetsplanering är att förutse och förebygga kapacitets- och prestandaproblem i KI:s IT-miljö. För att möjliggöra detta ska mätning och uppföljning av IT-kapaciteten genomföras regelbundet. För verksamhetskritiska IT-system inom KI ska kapacitetsplanering alltid ske.

Skydd mot skadlig kod

IT-utrusning som riskerar att drabbas av skadlig kod ska skyddas med lämplig programvara som ska vara kapabel att identifiera, ta bort och skydda mot kända typer av skadlig kod. Användare ska inte kunna avinstallera eller stänga av programvaran (antivirusfunktionen), utan detta ska endast kunna göras av behöriga administratörer. Uppdatering av programvarans definitionsfiler, liksom kontroll av utrustningen, ska ske automatiskt och kontinuerligt. Scanning av servrar och klienter efter skadlig kod ska utföras dagligen. Filer smittade av skadlig kod ska automatiskt oskadliggöras och händelser relaterade till skadlig kod ska loggas, larmas och följas upp.

Säkerhetskopiering och återläsning av data

Säkerhetskopiering av information och programvara ska genomföras regelbundet på sådant sätt att individuella filer kan återskapas. Frekvens och omfattning av säkerhetskopieringen varierar men bör baseras på de krav på tillgänglighet som definieras i informationsklassningen. Systemägaren är ansvarig för att, efter samråd med informationsägare, dokumentera dessa krav och säkerställa att lämpliga skyddsmekanismer finns på plats utifrån informationens klassning.

Säkerhetskopiorna ska vara tydligt märkta och skyddade mot överskrivning och fysisk förstörelse, och förvaras åtskilda ifrån originalen och i lokaler som följer kraven i *kapitel D4, Fysisk säkerhet*.

Återläsningstester ska genomföras regelbundet för att säkerställa att säkerhetskopiorna kan användas vid behov. Testresultaten ska dokumenteras.

Systemdokumentation

Det ska finnas fullständig och kontinuerligt uppdaterad systemdokumentation för alla IT-system inom KI. Systemdokumentation ska tas fram i enlighet med god praxis och dokumenterade, implementerade processer. Kopior av systemdokumentationen ska förvaras separerade från originalen, och arkivering av dokumentationen ska ske i enlighet med fastställda rutiner.
De delar av systemdokumentationen som behandlar känslig information, så som exempelvis säkerhetsfunktioner, ska förvaras så att endast behörig personal kommer åt dessa.

Kravställning av kommunikations- och nätverkssäkerhet

Karolinska Institutets IT-direktör ansvarar för övergripande kravställning rörande säkerheten avseende KI:s nätverk och infrastruktur.

B5. Styrning av åtkomst till information

Tillgång till information är nödvändigt för att kunna bedriva Karolinska Institutets verksamhet. Samtidigt är det viktigt att informationen endast är möjlig att komma åt för de personer som har ett faktiskt och berättigat behov av den. Känslig information måste skyddas från obehörig åtkomst och felaktiga förändringar. Det måste därför säkerställas att tillgång till information endast ges till behöriga personer.

Grundläggande säkerhet

Det är många individer, såväl medarbetare, studenter, uppdragstagare/anknutna, konsulter i verksamheten och till viss del leverantörer, som har åtkomst till KI:s information och system. Därför ska det finnas metoder och rutiner på plats för att kontrollera all åtkomst till information, system, nätverk och tjänster.

Det är också viktigt att alla som har åtkomst till KI:s IT-system beaktar informationssäkerhetsaspekterna och förstår sina personliga skyldigheter vid användandet av IT-system och hanteringen av information.

Åtkomst till information inom KI ska kontrolleras genom nedanstående administrativa och tekniska skyddsåtgärder.

Åtkomstadministration

För att säkerställa att endast behöriga användare har tillgång till viss information (både i digital och i fysisk form) ska åtkomsträttigheten godkännas av behörig person/roll innan den tilldelas en användare. Åtkomstens omfattning ska vid varje tillfälle avgränsas till användarens aktuella behov utifrån dennes arbetsuppgifter och organisatoriska tillhörighet. Detaljerade instruktioner avseende hur beställning, registrering, förändring och avregistrering av åtkomsträttigheter ska genomföras, ska definieras och dokumenteras.

Granskning av tilldelade åtkomsträttigheter ska genomföras regelbundet och åtgärder vidtas för att säkerställa att endast vid var tid behöriga användare har åtkomst till respektive informationstillgång/-system.

Åtkomstkontroll

Alla användare ska identifieras och verifieras genom användarnamn och lösenord innan de får åtkomst till ett system. För åtkomst till information som informationsklassats till den högsta nivån avseende konfidentialitet krävs flerfaktorsautentisering. Alla användare ska ha en unik identitet och alla användarkonton ska vara spårbara till en fysisk person.

Loggning och övervakning

För att säkerställa att alla användaraktiviteter är spårbara ska loggning ske på alla verksamhetskritiska IT-system. Detaljerade instruktioner och arbetssätt för uppföljning av loggar och hur eventuella överträdelser ska hanteras ska vara definierade och dokumenterade.

Anvisning för åtkomstadministration

För åtkomst till Karolinska Institutets (KI) nätverk och IT-system ska det finnas detaljerade instruktioner och en organisation för administration av åtkomsträttigheter. Detta för att säkerställa att det endast är godkända åtkomsträttigheter som läggs upp i systemen.
Systemägaren, eller motsvarande roll för de fall att information inte lagras i ett specifikt IT-system (utan exempelvis i en mappstruktur på gemensam lagringsyta), är ansvarig för instruktion och organisation för respektive system/miljö.

Vid administration av åtkomsträttigheter gäller följande:

- En behovs- och riskanalys ska göras gällande uppsättningen av åtkomsträttigheter i IT-systemet, eller annan elektronisk lagringsyta. Detta för att kunna tilldela rättigheterna på ett korrekt sätt. Analyserna ska genomföras och utvärderas i samråd med informationsägare.

- De åtkomsträttigheter som tilldelas en användare i ett system, eller annan elektronisk lagringsyta, ska inte vara högre än vad som krävs för att denne ska kunna utföra sina aktuella arbetsuppgifter.
- Åtkomsträttigheter till system, eller annan lagringsyta, får endast användas för att utföra de arbetsuppgifter som användaren är ålagd av KI att utföra.
- Om det finns flera ägare till information som behandlas i ett och samma IT-system ska dessa gemensamt komma överens om arbetssätt och instruktioner för åtkomstadministration.
- Användaridentiteter ska vara unika och användas i kombination med personliga lösenord.
- Höga åtkomsträttigheter, så kallade administratörsrättigheter, ska vara personliga och begränsas till så få personer som möjligt. Dessa får endast delas ut efter skriftligt beslut från respektive systemägare, eller motsvarande roll i de fall information inte lagras i ett specifikt system.
- Höga åtkomsträttigheter, så kallade administratörsrättigheter, för teknisk IT-utrustning ska vara personliga och begränsas till så få användare som möjligt och åtkomster får endast delas ut efter skriftligt beslut från respektive informationsägare.
- För åtkomst till information som informationsklassats till den högsta nivån avseende konfidentialitet krävs tvåfaktorsautentisering.
- Lösenord är personliga och ska hållas hemliga. Lösenord ska hanteras enligt gällande regelverk för lösenord inom KI.

Instruktioner för åtkomstadministration
Instruktion för kontroll över beställning, förändring och borttagande av åtkomsträttigheter ska fastställas för varje system, eller övrig elektronisk lagringsyta.

Anvisning för granskning av åtkomsträttigheter
Befintliga åtkomsträttigheter i KI:s IT-system och IT-miljöer ska regelbundet följas upp i syfte att säkerställa att de är förenliga med användarnas behov och arbetsuppgifter och att inte obehöriga har åtkomst till känslig information.

Granskningarna ska genomföras med olika frekvens baserat på informationsklassning enligt följande:

Informationsklass:	**Frekvens:**
K3 och/eller R3	Kvartalsvis
K2 och/eller R2	Kvartalsvis
K1 och/eller R1	Halvårsvis
K0 och/eller R0	Årligen

Behörigheter för särskilda privilegierade åtkomsträttigheter, s.k. administratörsrättigheter, ska alltid granskas minst kvartalsvis. Utöver ovan beskrivna frekvens ska granskningar av alla åtkomsträttigheter även ske vid större organisations- och systemförändringar.

Dokumentation
Då granskningar genomförs är det viktigt att dokumentationen sparas, både för att kunna följa upp hantering kring åtkomsträttigheter men även för att kunna visa för revisorer och annan tillsynsverksamhet att granskningarna verkligen har genomförts.

Nedanstående punkter ger en vägledning kring vilken typ av dokumentation som ska sparas som ett minimum:

- Underlag (användarlista från IT-systemet) som granskningen baserats på.
- Godkännande/bekräftelse avseende IT-systemets alla tilldelade åtkomsträttigheter.
- Underlag för beställning avseende förändring och borttagande som granskningen genererat.
- Nytt underlag (användarlista från IT-systemet) som visar att förändringar från granskningen har genomförts.

Generell vägledning för granskning av åtkomsträttigheter

OBS! Nedanstående vägledning är generell, förenklad och framtagen för att passa de flesta system, eller annan elektronisk lagringsplats, inom KI. Vägledningen är tänkt som ett stöd vid framtagandet av lokala instruktioner för att säkerställa att regelbunden och ändamålsenlig granskning av åtkomsträttigheter sker.

Regelbundna granskningar av åtkomsträttigheter bör minst innefatta följande aktiviteter:

1. Informationsägare, eller systemägaren om aktuell arbetsuppgift har blivit delegerad till denne, initierar granskningen genom att be relevant administratör att beställa/ta fram en lista över det aktuella IT-systemets användare och dess åtkomsträttigheter.
2. Listan med behörigheter skickas därefter till relevanta chefer, prefekter, administrativa chefer och eventuella andra intressenter (t.ex. informationsägare) vilka således involveras i granskningen genom att de granskar alla konton (både användarkonton och systemkonton) i IT-systemet utifrån följande aspekter:
    a. Vem är ägare av kontot?
    b. Har den personen behov av ett konto utifrån sina arbetsuppgifter?
    c. Är det rätt nivå på åtkomsträttigheter baserat på personens arbetsuppgifter och organisatorisk tillhörighet?
3. Administratören av granskningen sammanställer informationen från verksamhetens genomgång och tar därefter fram en förteckning över de förändringar och/eller borttagande av åtkomsträttigheter som ska göras.
4. Administratören genomför förändringarna alternativt beställer dem från IT-leverantören.
5. Administratören beställer/tar fram en ny lista över IT-systemets åtkomsträttigheter och säkerställer att de beställda förändringarna verkligen har genomförts.
6. Administratören slutför granskningen genom att spara den dokumentation som granskningen genererat på därför angiven plats.

Anvisning för loggning och loggranskning

Loggning ska ske på alla IT-system och lagringsplatser (exempelvis då forskningsdata inte lagras i ett specifikt IT-system utan till exempel i en mappstruktur på gemensam lagringsyta) där känslig information lagras eller på system som tillhandahåller verksamhetskritiska funktioner. Detta för att säkerställa att relevanta användaraktiviteter och informationssäkerhetshändelser registreras och är spårbara. Informationsägaren ansvarar för att säkerställa att tillfredsställande loggning och loggranskning sker gällande hantering av informationen. Systemägaren, eller motsvarande roll för

de fall att information inte lagras i ett specifikt IT-system (utan exempelvis i en mappstruktur på gemensam lagringsyta), ansvarar för att de faktiska granskningarna genomförs.

Loggning

Vid loggning gäller följande:

- Övervakning och loggning ska följa vid var tid gällande relevanta lagkrav. Loggarna ska åtminstone innehålla uppgifter om följande:
    - Samtliga händelser i IT-systemet, eller i annan elektronisk lagringsplats, initierade av en användare eller ett annat system.
    - Vilken användare som initierat händelsen och tidpunkten.
    - Samtliga misslyckade inloggningsförsök i IT-systemet samt vilken IP-adress varifrån inloggningsförsöket gjordes.
    - Systemlarm eller fel.
    - Ändringar, eller försök till ändringar, i IT-systemets säkerhetsuppsättningar och säkerhetsåtgärder.
- Användarna ska informeras om att deras aktiviteter i nätverk och IT-system etc. loggas och i vilket syfte dessa loggar följs upp. Denna information kan exempelvis ges i respektive systems användarinstruktioner eller som automatiskt meddelande i samband med inloggning.
- Samtliga loggfiler ska skyddas mot obehörig åtkomst och manipulation samt omfattas av relevant säkerhetskopiering i enlighet med fastställda instruktioner. Loggar ska sparas i enlighet med vid var tid gällande lagstiftning och informationsägares krav.
- För att säkerställa loggarnas bevisvärde ska loggande systems systemklockor synkroniseras med ett utpekat normalur.

Granskning av loggar

System som är högt klassade vad avser konfidentialitet (K2 och K3) och riktighet (R2 och R3) ska loggranskning genomföras regelbundet. Granskningarna ska genomföras utifrån fastställda instruktioner enligt följande:

- Instruktionerna ska beskriva vad som loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som betraktas som överträdelse och hur eventuella överträdelser ska hanteras och rapporteras. Beslut om hur ofta loggarna, i sin helhet eller endast vissa delar, ska granskas bör baseras på förekommande risker. Bedömningen bör bland annat ta hänsyn till värdet och känsligheten av aktuell information. Systemadministratörers aktiviteter bör dock granskas minst månatligen.
- Om möjligt ska loggarna analyseras med hjälp av automatiserade verktyg. Om detta inte är möjligt ska tillräckliga manuella kontroller i stället utföras.
- Tillgång och åtkomst till logg och logganalysverktyg ska begränsas och regleras med individuell åtkomsttilldelning.

Underlag från genomförda loggranskningar ska sparas och åtkomst till dessa regleras med individuell åtkomsttilldelning.

B6. Anskaffning, utveckling och underhåll av system

Karolinska Institutets IT-system och den information som hanteras där är av största vikt för verksamheten. För att säkerställa att känslig information hanteras på ett säkert sätt är det viktigt att IT-systemen har rätt funktionella och tekniska förutsättningar. Därför måste säkerhetskraven återspeglas i IT-systemen och hanteras redan vid planeringen av inköp eller utveckling av system.

Grundläggande säkerhet

Att ta hänsyn till och bygga in säkerhet i IT-system innan eller samtidigt som de utvecklas är generellt mer kostnadseffektivt och säkert än att tillföra säkerheten efteråt. För IT-system som hanterar personuppgifter finns det även ett krav i GDPR att dessa måste ha en inbyggt skydd för personuppgifterna som IT-systemet hanterar. Under utvecklingsprocessen bör kontinuerliga säkerhetstester genomföras för att i ett tidigt skede upptäcka sårbarheter och brister i IT-systemet.

I förberedelserna för utveckling eller upphandling av IT-system är det viktigt att säkerställa att informationssäkerhetens att riskanalyser och informationsklassningar genomförs. Detta för att säkerheten ska bli en integrerad del av IT-systemet vilket kräver ett strukturerat tillvägagångssätt och att kraven avseende informationssäkerhet är tydligt definierade. Därför ska en dokumenterad utvecklingsmetod eller ett dokumenterat anskaffningssätt som tar hänsyn till detta användas.

God kunskap om verksamhetens krav och informationssäkerhetskrav är väsentligt om IT-systemet ska kunna uppfylla sitt syfte. Utvecklingen eller upphandlingen ska minst beakta följande:

- Tvingande myndighetskrav
- Interna regler avseende informationssäkerhet
- Driftstabila och beprövade lösningar

En strikt och väldefinierad arbetsrutin krävs när nya IT-system eller utvecklade system-komponenter implementeras från utvecklings- och testmiljön in i produktionsmiljön. Vid implementering av nya komponenter eller nya funktioner ska en riskanalys göras. Endast formellt accepterade och godkända IT-system eller systemkomponenter får implementeras i produktionsmiljön.

För att upprätthålla en säker och tillförlitlig tillgång till information ska administration, drift och underhåll av IT-system ske på ett strukturerat och systematiskt sätt enligt formaliserad och antagen modell för systemförvaltning. Systemägaren för respektive IT-system ansvarar för att ställa krav avseende systemförvaltningen.

Anvisning för kravställning vid anskaffning och utveckling av system

Vid utveckling eller anskaffning av IT-system ska informationsägare säkerställa att nedanstående aktiviteter genomförs:

Innan utveckling eller anskaffning

- En informationsklassning och riskanalys ska genomföras för att definiera de informationssäkerhetskrav som ställs på IT-systemet. Dessa krav ska sedan dokumenteras som en del av kravspecifikationen.
- I samband med riskanalysen ska även en bedömning göras hur den tilltänkta systemlösningen förhåller sig till lagar och förordningar, till exempel GDPR.

Upphandling av leverantör för utveckling eller anskaffning

- Vid upphandling av IT-system ska dokumenterade krav på leverantörernas informationssäkerhets- och dataskyddsarbete ingå i förfrågningsunderlaget.
- KI:s krav på informationssäkerhet och dataskydd ska definieras och avtalas med utvald leverantör.
- Om upphandlingen innefattar att leverantören kommer att behandla personuppgifter på KI:s räkning ska ett personuppgiftsbiträdesavtal upprättas mellan parterna.
- Vid systemutveckling ska en bedömning göras över vilken programvara, information och vilka rättigheter som ska ägas av KI efter uppdragets slut. Vidare ska det bedömas vilka rättigheter leverantören har och vilken information denne har tillgång till, särskilt för känsliga personuppgifter. Avtal med vald leverantör ska utformas enligt denna bedömning.

Under utveckling eller anskaffning

- Vid utveckling ska vedertagna systemutvecklingsmodeller användas för att säkerställa spårbarheten i utvecklingens alla led.
- Tester ska genomföras i separat testmiljö för att säkerställa riktigheten i IT-systemets utdata. Testdata ska alltid vara anonymiserad och faktiska personuppgifter får aldrig användas i testsammanhang**.** Utdatas riktighet ska utvärderas under testfasen med hjälp av rimlighetskontroller.
- Det ska säkerställas att identifierade säkerhetskrav för IT-systemet implementerats i enlighet med vad som definierats i kravspecifikationen.
- Innan IT-systemet får sättas i produktion ska det genomgå acceptanstest/validering som beställaren ska godkänna.
- En systemägare ska utses för IT-systemet.

Produktionssättning av utvecklat eller anskaffat system

- I beställarens driftgodkännande, som ska ligga till grund för beslut gällande produktionssättning av IT-systemet, ska det ingå en uppföljning över de fördefinierade informationssäkerhetskraven.
- Vid utveckling eller anskaffning ska fullständig system-, användar- och drifts-dokumentation framställas. Driftsdokumentationen ska även översiktligt behandla de återstartsrutiner som behövs för IT-systemets avbrottsplanering. All dokumentation ska vara färdigställd och tillgänglig för berörda personer senast vid produktionssättning av IT-systemet.

Anvisning för kravställning av systemförvaltning

För att upprätthålla en säker och tillförlitlig tillgång till information ska administration, drift och underhåll av IT-system ske på ett strukturerat och systematiskt sätt enligt en formaliserad och antagen modell för systemförvaltning. Systemägaren för respektive IT-system ansvarar för att ställa krav avseende systemförvaltningen.

Systemägaren ansvarar själv, eller genom särskilt utsedd systemförvaltare, för förvaltningen av IT-systemet och de säkerhetskrav som är relaterade till förvaltningen. Systemägaren ansvarar för att åtminstone, men inte uteslutande, nedanstående krav uppfylls inom ramen för förvaltningen av IT-systemet.

- Det ska finnas en dokumenterad förvaltningsplan, innehållande instruktioner för administration, drift och underhåll, i syfte att säkerställa att IT-systemet hanteras korrekt utifrån ett informationssäkerhetsperspektiv.
- Det ska finnas aktuell och uppdaterad systemdokumentation vilken ska vara tillgänglig för berörda och behöriga personer vid behov.
- Det ska finnas en avbrottsplan för IT-systemet och planen ska vara kopplad till kontinuitetsplanerna för de verksamhetsområden som IT-systemet stödjer.
- Det ska genomföras en systemklassning som baseras på den information som hanteras i IT-systemet. En översyn av befintlig klassning ska genomföras årligen samt vid varje större förändring i IT-systemet, eller förändringar av den information som IT-systemet hanterar.
- Det ska tillföras medel i budgeten för att eventuella säkerhetsbrister som identifieras genom t.ex. arbetet med systemklassning och riskanalyser kan åtgärdas.
- IT-systemets användare ska informeras om IT-systemets skyddsåtgärder och användarna ska erhålla nödvändig säkerhetsutbildning innan de tillåts åtkomst till IT-systemet.
- Alla informationssäkerhetsincidenter som uppdagas inom ramen för förvaltningen ska rapporteras skyndsamt i enlighet med vid var tid gällande anvisningar. För ytterligare information kring incidentrapportering se *avsnitt B8, Incidenthantering.*
- Samtliga IT-system ska säkerhetsgranskas kontinuerligt och funktionella fel och brister relaterat till IT-systemet ska kontinuerligt analyseras och rapporteras till systemägaren.
- Då förändringar görs i IT-systemet ska alltid KI:s informationssäkerhetskrav avseende förändringshantering följas.

Systemförvaltaren ska, utöver den praktiska hanteringen av ovanstående ställda krav, bistå system- och informationsägaren avseende:

- Hanteringen av åtkomstadministration och granskning av åtkomsträttigheter.
- Riskanalyser samt framtagande av åtgärds- och förbättringsförslag baserade på dessa.

Anvisning för kravställning vid drift utanför Karolinska Institutet

Då KI köper tjänster eller förlägger drift av IT-resurser utanför den egna organisationen ska samma regler avseende informationssäkerhet gälla som när driften hanteras i egen regi. Utöver detta ska även följande regler gälla då drift sker utanför KI:

- Kraven på informationssäkerhet ska definieras baserat på en dokumenterad informationsklassning och riskanalys och regleras i avtal parterna emellan. Systemägaren ansvarar för kravställning och uppföljning av dessa krav, men samordning bör ske i de fall leverantören hanterar flera av KI:s IT-resurser.
- Då systemanskaffning, utveckling eller underhåll ingår i den externa partens åtagande ska säkerhetskraven i *Anvisning för kravställning vid anskaffning och utveckling av IT-system* följas.
- Uppföljning av avtalade säkerhetskrav ska ske regelbundet. Detta ska möjliggöras genom att i avtalet specificera att KI har rättighet att genomföra revision och granskning av den tillhandahållna tjänsten och hur väl leverantören uppfyller gällande och relevanta informationssäkerhetskrav.

- Om informationen i IT-systemen innehåller personuppgifter ska parternas roller som personuppgiftsansvarig och personuppgiftsbiträde regleras i avtal. I avtalet ska det specificeras att personuppgiftsbiträdet endast får behandla personuppgifterna i enlighet med instruktioner från den personuppgiftsansvarige. Utöver detta måste personuppgiftsbiträdet även vidta lämpliga och tillräckliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.
- Risker som följer av beroende till en viss leverantör ska minimeras.

Molntjänster

Drift av IT-system som innehåller känslig information, alternativt behöver integreras med andra system, ska inte upphandlas som en molntjänst utan att en noggrann informationsklassning och riskanalys först har genomförts och dokumenterats. Utifrån analysernas resultat ska nödvändiga åtgärder vidtas och minst följande ska säkerställas:

- Garantier på tillgänglighet ska finnas med i avtalet med leverantören. Tillgängligheten ska motsvara verksamhetens krav.
- Om tillgänglighetskraven är höga ska det finnas en redundant internetförbindelse.
- Avtalet bör innehålla en vitesklausul.
- Avtalet ska specificera vilken eller vilka organisationer som har tillgång till informationen.
- Antalet personer som har tillgång till informationen ska vara begränsat.
- Avtalet ska uttryckligen specificera att leverantören ***inte*** få använda sig av KI:s information för eget eller annan parts bruk utöver vad som specifikt är avtalat.
- Om informationen kommer att hanteras utanför Sverige ska rättsläget vara analyserat och det ska säkerställas att säkerhetskraven för till exempel personuppgifter kan garanteras.
- Funktioner för att exportera data ska finnas i tjänsten så att KI vid avtalsslutet, eller i övrigt vid behov, lätt kan byta leverantör.
- Avtalet ska specificera KI:s revisionsmöjligheter så att uppföljning av avtalade säkerhetskrav möjliggörs.

B7. Hantering och rapportering av incidenter

En incident är en händelse som kan få negativ påverkan på Karolinska Institutets verksamhet. Informationssäkerhetsincidenter kan till exempel vara förlust av, eller obehörig åtkomst till, information, stöld av IT-utrustning eller datavirusutbrott m.m. För att minska risken att KI:s verksamhet påverkas vid en incident är det viktigt att alla vet hur man ska agera och vart man ska vända sig för att rapportera avvikande händelser och inträffade informationssäkerhetsincidenter.

Grundläggande säkerhet

För att säkerställa att eventuella informationssäkerhets- och personuppgiftsincidenter får minimal påverkan på KI:s verksamhet ska det finnas en formaliserad process för rapportering och hantering av incidenter. Det ska genom denna process säkerställas att incidenter och svagheter relaterade till informationshantering blir rapporterade på ett sådant sätt att lämpliga åtgärder kan vidtas på kort och lång sikt.

Informationssäkerhetsincidenter är händelser som påverkar, eller kan komma att påverka, säkerheten negativt för KI:s informationstillgångar. Incidenter som på något sätt innefattar

personuppgifter klassas som personuppgiftsincident. En incident kan antingen bero på ett avsiktligt eller ett oavsiktligt agerande. Den gemensamma nämnaren är att informationssäkerheten hotas genom t.ex. obehörig åtkomst till information, olaglig hantering av data, felaktighet i information, driftavbrott eller brist på tillgång till information.

Exempel på incidenter kan vara obehörig eller oetiskt användande av information, dataintrång och skadlig kod (s.k. virus). Ytterligare exempel är förlorad information i pappersform, förlust av dator eller annan lagringsmedia.

Samtliga verksamma ska känna till vad som klassas som en incident samt var och hur dessa ska rapporteras. Rapporterade incidenter ska klassas enligt definierad incidentmodell utifrån potentiell påverkan på information, individer och verksamheten. Incidenterna ska hanteras i prioritetsordning i relation till den klass som incidenten tilldelas. För detaljerad information om rapportering av incidenter, se anvisningarna nedan.

Alla inrapporterade incidenter ska efter hantering analyseras med avseende på orsak och påverkan. Detta då det kan finnas ett samband mellan olika incidenter som inte är direkt synligt. Ett antal mindre incidenter kan tillsammans visa på omfattande säkerhetsbrister som är svåra att identifiera utan en genomgående analys. Identifierade säkerhetsbrister definieras som incidenter och ska rapporteras och hanteras enligt ovan.

Vid incidenter som bedöms kunna få mycket stor påverkan på KI:s verksamhet ska KI:s säkerhetschef omedelbart informeras i syfte att kunna aktivera KI:s övergripande kris- och katastrofplan om detta bedöms som nödvändigt.

Anvisning för rapportering och hantering av informationssäkerhets- och personuppgiftsincidenter

Rapportering av incidenter

Informationssäkerhets- och personuppgiftsincidenter ska alltid rapporteras skyndsamt, bl.a. i syfte att begränsa skadeverkningar och främja utredningsmöjligheter, men också för att KI har en tidsfrist på 24 h från upptäckt, för rapportering av allvarliga IT-incidenter till MSB, respektive 72 h från upptäckt av personuppgiftsincidenter till Datainspektionen. Rapportering av incidenter till berörda tillsynsmyndigheter görs av KI:s centrala säkerhetsfunktioner (IT-säkerhet/informationssäkerhet) eller dataskyddsombud (om personuppgiftsincidenter).

Rapportering ska primärt ske via systemstöd alternativt till institutionens prefekt eller av denne utsedd kontaktperson för informationssäkerhet. Detta gäller för såväl informationssäkerhetsincidenter som personuppgiftsincidenter.

Incidenthantering

IT-säkerhetsansvarig ska (eventuellt i samråd med informationssäkerhetsfunktionen) skyndsamt göra en första analys av incidentens potentiella påverkan för att bedöma hur den ska klassas och om den eventuellt ska eskaleras vidare i organisationen.

Som informations- och systemägare vid KI har man ett utökat ansvar att bistå vid utredningen av incidenter, framförallt gällande vad för typer av information som är föremål för incidenten. Dessa roller kan även bli kallade till möten för att göra en bedömning av incidentens potentiella konsekvenser.

Avrapportering

Systemägare ansvarar själva för, eller genom utsedd systemförvaltare, att årligen sammanställa samtliga incidenter kopplade till IT-systemet och rapportera dessa till den centrala

informationssäkerhetsfunktionen. Åtgärdsbehov som inträffade incidenter medfört ska tas om hand i förvaltningsplaner.

B8. Kontinuitetsplanering

Tillgång till Karolinska Institutets information är en grundförutsättning för att bedriva verksamheten. Vid avbrott i tillgång till information och systemstöd måste det finnas planer och rutiner på plats för att säkerställa att verksamheten trots allt kan fortsätta bedrivas.

Grundläggande säkerhet

Det huvudsakliga målet med kontinuitetsplanering för KI:s verksamhet är att säkerställa att eventuella avbrott i tillgången till information och systemstöd inte får allvarliga konsekvenser för verksamheten. Det ska säkerställas att potentiella risker, avbrott och hot mot verksamhetens kontinuerliga drift har utvärderats och att lämpliga åtgärder har vidtagits. Dessa åtgärder ska vara tydligt strukturerade och organiserade för att tillgången till information och systemstöd ska kunna återställas inom för verksamheten definierad kritisk tid. Alla berörda parter ska veta hur, när och vilka olika åtgärder som ska vidtas då en incident i form av ett avbrott inträffar. Fokus för denna del av kontinuitetsplaneringen ligger på hantering av information och system. De delar av kontinuitetsplaneringen som berör katastrof- och beredskapssituationer ska ingå i KI:s övriga katastrofplanering som säkerhetschefen ansvarar för att ta fram och uppdatera.

Informationsägare är ansvariga för att, med hjälp av systemägaren, säkerställa att det finns en riskutvärdering och riskhantering på plats för IT-system där känslig information hanteras och att en avbrottsplan utvecklas och underhålls för nödvändiga delar. Riskanalyser och informationsklassningen utgör grunden i kravställningen av IT-systemet avseende kontinuitet. Verksamhetskritiska IT-system har högre skyddskrav och kraven på dess kontinuitet är också högre. All verksamhet och alla IT-system är sannolikt inte lika kritiska för att verksamhet ska kunna bedrivas och det är därför fullt möjligt att besluta om att vissa IT-system inte täcks av någon kontinuitetsplan och att resurser och insatser, i händelse av en akut situation, i stället primärt fokuseras på mer verksamhetskritiska aktiviteter och IT-system. Således kommer dessa oprioriterade IT-system hanteras först när de kritiska IT-systemen har återställts.

Förvaltningsledare ska upprätta avbrottsplaner att använda vid större avbrott och som ska innehålla t.ex. ansvarsförhållanden, kontaktpersoner och eskaleringsvägar till interna och externa aktörer. För att uppnå en god kontinuitet krävs en kombination av förebyggande och återställande skyddsåtgärder. Under arbetet med att ta fram kontinuitetsplaner identifieras ofta ett antal åtgärder som minskar risken för att katastrofsituationer, störningar och oplanerade avbrott överhuvudtaget ska inträffa. I KI:s verksamheter som är mycket känsliga för avbrott bör stort fokus läggas på dessa förebyggande åtgärder.

Kontinuitets- och avbrottsplaner ska uppdateras kontinuerligt och övningar ska ske regelbundet, minst årligen, för att säkerställa att de fungerar, är ändamålsenliga och fortfarande speglar den aktuella situationen. Test av planerna fungerar även som utbildnings- och kommunikationsinsats för berörda funktioner och roller.

Anvisning för kontinuitetsplanering

Kontinuitetsplanering ska ske för KI:s alla institutioner och dess kritiska verksamhetsdelar och dokumenteras i en kontinuitetsplan. Följande områden ska beaktas:

1. **Definition av områden/omfattning och strategi**
   Kontinuitetsplanen ska tydligt ange vilka verksamhetsdelar den täcker och den valda strategin för att återställa dessa. Det kan finnas olika strategier beroende på typ av

händelse som får konsekvens för verksamhetsdelens tillgänglighet, samt vilken del planen avser att täcka. Risk- och konsekvensanalyser ska genomföras och bilda grund för den valda strategin.

2. **Risk- och konsekvensanalyser**
   Riskanalyser, som beaktar potentiella sårbarheter och hot för verksamheten och dess nyckeldelar, ska genomföras regelbundet (för mer information se Anvisning Genomförande av riskanalyser). Genom riskanalysarbetet inhämtas information som är nödvändig för att bland annat kunna ta fram en relevant kontinuitetsplan och genomföra förebyggande arbete. I kontinuitetsplaneringen ska riskanalysen även innefatta en konsekvensanalys, där fokus ska ligga på konsekvenserna av bristande tillgänglighet till kritisk information. På så sätt identifieras verksamhetens behov av, och krav på tillgänglighet till, information i syfte att kunna upprätthålla kritiska verksamhetsdelar.

3. **Återställningstider**
   Utifrån resultatet av konsekvensanalysen ska kritiska återstartstider för väsentliga verksamhetsdelar definieras. Fastställande av återstartstider innebär att den maximala tid som aktuell verksamhetsdel tillåts vara otillgänglig ska definieras. Denna tid får i sin tur påverkan på utformningen av de kontinuitetslösningar, åtgärdsaktiviteter och reservrutiner som ska dokumenteras i kontinuitetsplanen.

4. **Kontinuitetslösningar**
   De definierade återställningstiderna utgör underlag för vilka kontinuitetslösningar som ska väljas och hur reservrutinerna ska utformas. Lösningarna för att uppnå kontinuitet i verksamheten ska utformas så att de är praktiskt och ekonomiskt genomförbara utifrån vald strategi. Utformningen av reservrutinerna ska vara så detaljerad att den kan ligga till grund för kontinuitetsplaneringen.

5. **Organisation för att utarbeta, införa och underhålla planen**
   Roller och ansvar för att ta fram och kontinuerligt arbeta med kontinuitetsplanerna ska definieras och kommuniceras. Arbetet med och ansvaret för detta kan med fördel delas upp relaterat till de olika verksamhetsdelar som ska täckas av kontinuitetsplanering. Det är dock viktigt att det finns en utsedd ansvarig person som ansvarar för förvaltning och underhåll av den övergripande kontinuitetsplanen.

6. **Granskning, test och övning**
   Kontinuitetsplaner behöver underhållas, och som en del av detta arbete ingår att planerna regelbundet granskas och uppdateras. Regelbundna övningar av planerna ska också genomföras för att på så sätt testa att de är aktuella, ändamålsenliga och att de verkligen fungerar när de behövs. Dessa övningar fungerar även som utbildning i kontinuitetsplanernas reservrutiner för medarbetare och andra berörda.

Kapitel C: Informationssäkerhet för IT-verksamhet och den IT-nära förvaltningen

Kapitel C innehåller regler och anvisningar för informationssäkerhet som rör målgruppen IT-verksamhet på KI. Detta gäller oavsett om man arbetar med IT på en institution, IT vid Universitetsförvaltningen (UF) eller om man är IT-konsult. Utöver det som presenteras i kapitlen nedan ska IT-verksamheten vid KI arbeta efter de säkerhetskrav som informations- och systemägare vid KI ställer mot IT-verksamheten.

För ansvarsbeskrivningar för dessa roller se Bilaga 1, Informationssäkerhetsorganisation och ansvarsbeskrivningar.

C1. Ansvarsbeskrivning IT-verksamhet

Ansvar för informationssäkerhet och IT-säkerhet inom IT-verksamheterna vid KI följer ordinarie verksamhetsansvar. Det innebär att chefer och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av informations- och IT-säkerhet för de processer och de IT-resurser de ansvarar för.

På ITA ligger informationssäkerhetsansvaret ytterst på IT-direktören i egenskap av chef för avdelningen. Det innebär att säkerheten i informationshantering och IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt dessa riktlinjer, regler och anvisningar för informationssäkerhet.

IT-verksamheterna på KI ansvarar inom informationssäkerhetsområdet bl.a. för att:

- Följa gällande regler för informationssäkerhet.
- Säkerställa efterlevnad avseende de informationssäkerhetskrav som ställs specifikt på system, miljöer och komponenter. Kraven är ofta resultat av informationsklassning och riskanalyser som informations- och systemägare ansvarar för och kan vara av teknisk karaktär, men också organisatorisk och administrativ.
- Inom vissa områden i IT-miljön behöver mer detaljerade anvisningar och instruktioner tas fram som kompletterar eller konkretiserar dessa riktlinjer. IT-verksamheterna vid KI ansvarar för att utforma dessa och de ska baseras på KI:s regler och anvisningar avseende informationssäkerhet. Anvisningarna ska hållas uppdaterade och följas.
- Säkerställa att anlitade leverantörer och konsulter inom IT-området uppfyller KI:s krav på informationssäkerhet.

C2. Hantering av tillgångar

På Karolinska Institutet finns tillgångar som är nödvändiga för den verksamhet som bedrivs, t.ex. informationstillgångar i form av forsknings- och utbildningsdata. Dessa tillgångar måste hanteras på sådant sätt att det går att säkerställa att de skyddas mot obehörig åtkomst, felaktiga förändringar och att de finns tillgängliga då de behövs.

Identifiering av IT-resurser och tilldelning av ägare

Samtliga IT-resurser vid KI, såväl lokalt som centralt, ska vara identifierade och en förvaltningsorganisation ska finnas upprättad.

Varje verksamhet, UF, institutioner och likvärdiga, ansvarar för att en förteckning över att den egna verksamhetens alla IT-resurser upprättas och underhålls.

Klassning av IT-resurser

Det är IT-resursernas systemägare som genom kravställning mot IT-verksamhet ansvarar för att säkerhetsnivån är tillräcklig. Systemägaren ansvarar för att IT-resurserna klassas i enlighet med KI:s modell för systemklassning. Klassningen görs bl.a. annat för att klargöra hur betydande resursen är för verksamheten och vilka krav på säkerhetsåtgärder och hantering som gäller.

Systemklassningen bygger på vilken information som hanteras i IT-resursen och hur den är klassad, s.k. informationsklassning. Ansvariga för informationsklassning är *Informationsägare*. De som arbetar inom IT-verksamheten på KI kan däremot i vissa fall behöva bistå vid själva klassningen. Klassningen resulterar i både administrativa och tekniska åtgärder varpå IT-verksamheten har ett ansvar för att införa de tekniska skyddsåtgärderna på begäran av informations- eller systemägaren. För mer information om klassning, se avsnitt *B2, Informations- och systemklassning*, samt informationssäkerhetssidan på medarbetarportalen.

C3. Riskhantering

Den information och de IT-system som används inom KI är viktiga för att bedriva verksamheten och måste skyddas på lämpligt sätt. För att avgöra hur KI ska skydda information och IT-system på rätt sätt måste relaterade risker identifieras och analyseras. Riskanalyser ska vara en naturlig del av KI:s arbetssätt och bidra till att verksamheten kan bedrivas på ett ändamålsenligt och effektivt sätt.

Grundläggande säkerhet

För att säkerställa att information hanteras på ett säkert sätt ska hot och risker relaterade till information kontinuerligt identifieras, analyseras och hanteras med lämpliga skyddsåtgärder. För att komma fram till vilka skyddsåtgärder som är lämpliga för respektive informationstillgång ska riskanalyser genomföras kontinuerligt. För IT-verksamheten handlar detta främst om att identifiera risker för de IT-system som används vid KI.

Riskanalyser gör det möjligt för informations- och systemägare att identifiera huvudsakliga risker. Dessa bedöms sedan utifrån hur stor sannolikheten är att hoten realiseras samt potentiella konsekvenser. Analysen ger underlag för att avgöra vilka skyddsåtgärder som krävs för att säkerställa att riskerna, dvs. konsekvensen och sannolikheten för att ett hot inträffar, hanteras och minimeras på lämpligt sätt. Alla skyddsåtgärder ska dokumenteras på ett sådant sätt att det är möjligt att kontrollera efterlevnaden.

Inom KI ska riskanalyser vara en naturlig del av hanteringen av information och genomföras på flera olika nivåer; på övergripande organisationsnivå, på institutionsnivå, avseende specifika IT-system eller informationstillgångar etc. Riskanalyser ska utgå från aspekterna konfidentialitet, riktighet och tillgänglighet för den analyserade informationen. Riskanalyser ska genomföras i samband med förändringar i verksamheten, processerna och systemen. För alla verksamhetskritiska IT-system ska riskanalyser genomföras årligen. I samband med detta ska det även analyseras om det finns nya, eller förändrade, interna eller externa krav som påverkar det aktuella IT-systemet. Till alla identifierade risker ska det utses en ansvarig som svarar för att säkerställa att de hanteras på ett lämpligt sätt. Uppföljning ska ske av att identifierade risker åtgärdas, alternativt hanteras på annat sätt, inom en rimlig tid.

Resultatet från genomförda riskanalyser ska rapporteras till säkerhetschefen via informationssäkerhetssamordnaren.

Anvisning för genomförande av riskanalyser

I enlighet med KI:s regler och riktlinjer för intern styrning och kontroll, ska riskanalyser genomföras regelbundet på olika nivåer och olika områden inom KI:s verksamhet. Det finns olika metoder och modeller för att genomföra riskanalyser. Inom KI finns en beslutad riskanalysmetod som företrädesvis ska användas. Oavsett vilken metod som används ska nedanstående aktiviteter alltid utföras vid genomförandet av en riskanalys.

1. **Analysens omfattning och avgränsning ska definieras**
   Ramarna för den riskanalys som ska genomföras sätts genom att det område eller den process som ska analyseras definieras och avgränsas. Riskanalysmetod ska väljas och personer med god kännedom om aktuellt område/process ska identifieras och bjudas in att delta i analysen. Dessa personer ska också ges tillfälle att förbereda sig och inhämta nödvändig information/fakta för att kunna genomföra uppgiften på ett effektivt och ändamålsenligt sätt.

2. **Hot ska identifieras**
   För varje delområde, eller steg i processen, som analyseras ska de hot som föreligger identifieras, grupperas och dokumenteras. Hoten ska dokumenteras på tillräcklig detaljnivå så att även utomstående förstår vad som avses.

3. **Konsekvens och sannolikhet ska bedömas**
   Vilka konsekvenserna blir om identifierade hot inträffar, och hur sannolikt det är att de inträffar, ska identifieras, analyseras och resultatet dokumenteras. Omfattningen av risken, dvs. konsekvensen och sannolikheten för att ett hot inträffar, bör bedömas utifrån en definierad metod som också gör det möjligt att jämföra risker och deras omfattning.

4. **Åtgärdsförslag ska utarbetas**
   Det kan ligga flera olika orsaker bakom varje identifierad risk, och förslag för att hantera dessa måste därför arbetas fram. Konsekvensen av förslagen måste analyseras innan beslut om åtgärd fattas. Åtgärder kan exempelvis vidtas för att förhindra eller minska sannolikheten för att de bakomliggande orsakerna inträffar, eller att konsekvenserna av om de inträffar minimeras.

5. **Riskanalysen ska dokumenteras**
   En rapport ska sammanställas utifrån den genomförda riskanalysen. Rapporten bör, förutom själva analysresultatet och beskrivningen av de risker man funnit, innehålla information kring alla steg i genomförandet av riskanalysen. Rapporten bör även innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta beslut i frågan. Dessa förslag ska ligga till grund för planering av det fortsatta arbetet kring riskhanteringen.

6. **Handlingsplan ska tas fram och följas upp**
   En prioriterad handlingsplan, med angivande av vilka åtgärder som ska vidtas, vem som ansvarar för dessa och när de ska vara genomförda ska tas fram och följas upp. Föreligger det risker för vilka verksamheten bedömer att det inte behövs några åtgärder ska även denna accept av kvarvarande risker dokumenteras.

C4. Driftsäkerhet

Inom Karolinska Institutets verksamhet finns beroenden till olika system, och den information som hanteras där. Det är därför av stor vikt att dessa IT-system finns tillgängliga vid behov.

Grundläggande säkerhet

Systemägaren till en specifik IT-resurs (system/applikation, nätverk, teknisk plattform etc.) ansvarar för kravställning avseende dess driftsäkerhet, vilken omfattas av följande områden: säkerhetsuppdateringar, förändringshantering, kapacitetsplanering, skydd mot skadlig kod, säkerhetskopiering och återläsning av data samt system- och driftsdokumentation. Mer information kring detta finns nedan i *Anvisning för kravställning av driftsäkerhet och servicenivå*.

Då KI köper tjänster eller förlägger drift av IT-resurser utanför den egna organisationen ska samma regler avseende informationssäkerhet gälla som när driften hanteras i egen regi. Kraven på informationssäkerhet ska definieras baserat på en dokumenterad informationsklassning och riskanalys och kraven ska regleras i avtal parterna emellan.
Ägaren till den specifika IT-resursen ansvarar för kravställning och uppföljning av dessa krav, men samordning bör ske i de fall leverantören hanterar flera av KI:s IT-resurser. Mer information finns i *Anvisning för kravställning vid drift utanför Karolinska Institutet på sid 47.*

Om tjänsten eller driften av IT-resursen innefattar behandling av personuppgifter ska även ett personuppgiftsbiträdesavtal upprättas mellan parterna.

Anvisning för kravställning av driftsäkerhet och servicenivå

Nivå på kravställningen på specifika IT-resurser bör baseras på genomförd informationsklassning. Denna anvisning anger den miniminivå som ska följas inom Karolinska Institutet och utgör även ett stöd för att definiera vilka områden som exempelvis, men inte uteslutande, bör ingå i kravställningen.

Separerade miljöer

Produktions-, utvecklings-, test-, och utbildningsmiljöer bör vara separerade. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för utvecklings- och testmiljöerna.

Drift och driftsdokumentation

Drift av KI:s IT-resurser ska ske i enlighet med god praxis och dokumenterade, implementerade processer. Det ska finnas dokumenterade och kontinuerligt uppdaterade operationella driftsrutiner och driftsinstruktioner, och all drift ska ske i enlighet med dessa. Den dokumenterade driftsdokumentationen ska uppdateras vid behov och revideras minst årligen eller när behov i övrigt föreligger. Där så är möjligt ska bevis på att rutinerna/instruktionerna följs dokumenteras och lagras. Kopior av driftsdokumentationen ska förvaras separerade från originalen och arkivering av dokumentationen ska ske i enlighet med fastställda rutiner.

Säkerhetsuppdateringar

Säkerhetsuppdateringar avseende operativsystem och program ska hanteras kontrollerat och skyndsamt. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön. Om analysen påvisar att säkerhetsuppdateringen genererar risker för stabiliteten i produktionsmiljön ska en dokumenterad motivering finnas för varför säkerhetsuppdateringen inte genomförs.

Detaljerade anvisningar ska finnas för hantering av akuta säkerhetsuppdateringar, det vill säga säkerhetsuppdateringar som måste installeras så skyndsamt att de inte hinner testas. Instruktionerna bör säkerställa att tester genomförs efter installationen, och att åtgärder vidtas baserat på testernas resultat.

Förändringshantering

Alla förändringar som görs i KI:s IT-system ska noggrant planeras och analyseras, och alla förändringar, liksom test och överföring till produktionsmiljön av dessa, ska vara formellt godkända av behörig person. Godkännanden ska dokumenteras och lagras. Dualitetsprincipen bör tillämpas – det vill säga utveckling, test och produktionssättning bör inte ske av en och samma person och ska ske i separata miljöer. Utvecklings- och testmiljön får inte, utan att särskilda, av systemägaren godkända, säkerhetsåtgärder vidtagits, innehålla känslig information.

Det ska finnas detaljerade anvisningar för hur förändringar ska hanteras och testas, liksom planer för att, vid behov, kunna återgå till läget innan förändringen påbörjades.

Detaljerade anvisningar ska även finnas för akuta förändringar som måste åtgärdas omgående, och där tid inte finns för att följa den normala förändringsprocessen. Sådana förändringar kan exempelvis vara störningar i produktionsmiljön. Akuta förändringar ska dokumenteras och i efterhand följas upp enligt detaljerade anvisningar för akut förändringshantering.

Kapacitetsplanering

Syftet med kapacitetsplanering är att förutse och förebygga kapacitets- och prestandaproblem i KI:s IT-miljö. För att möjliggöra detta ska mätning och uppföljning av IT-kapaciteten genomföras regelbundet. För verksamhetskritiska IT-system inom KI ska kapacitetsplanering alltid ske.

Skydd mot skadlig kod

IT-utrusning som riskerar att drabbas av skadlig kod ska skyddas med lämplig programvara som ska vara kapabel att identifiera, ta bort och skydda mot kända typer av skadlig kod. Användare ska inte kunna avinstallera eller stänga av programvaran (antivirusfunktionen), utan detta ska endast kunna göras av behöriga administratörer. Uppdatering av programvarans definitionsfiler, liksom kontroll av utrustningen, ska ske automatiskt. Scanning av servrar och klienter efter skadlig kod ska utföras dagligen. Filer smittade av skadlig kod ska automatiskt oskadliggöras och händelser relaterade till skadlig kod ska loggas, larmas och följas upp.

Säkerhetskopiering och återläsning av data

Säkerhetskopiering av information och programvara ska genomföras regelbundet på sådant sätt att individuella filer kan återskapas. Frekvens och omfattning av säkerhetskopieringen varierar men bör baseras på de krav på tillgänglighet som definieras i informationsklassningen. Systemägaren är ansvarig för att, efter samråd med informationsägare, dokumentera dessa krav och säkerställa att lämpliga skyddsmekanismer finns på plats utifrån informationens klassning.

Säkerhetskopiorna ska vara tydligt märkta och skyddade mot överskrivning och fysisk förstörelse, och förvaras åtskilda ifrån originalen och i lokaler som följer kraven i *kapitel D4, Fysisk säkerhet*.

Återläsningstester ska genomföras regelbundet för att säkerställa att säkerhetskopiorna kan användas vid behov. Testresultaten ska dokumenteras.

Systemdokumentation

Det ska finnas fullständig och kontinuerligt uppdaterad systemdokumentation för alla IT-system inom KI. Systemdokumentation ska tas fram i enlighet med god praxis och dokumenterade, implementerade processer. Kopior av systemdokumentationen ska förvaras separerade från originalen, och arkivering av dokumentationen ska ske i enlighet med fastställda rutiner. De delar av systemdokumentationen som behandlar känslig information, så som exempelvis säkerhets-funktioner, ska förvaras så att endast behörig personal kommer åt dessa.

Förvaltningsledare ansvarar för att t.ex. systemklassning och planerade säkerhetsåtgärder dokumenteras och ingår i förvaltningsplaner. De ska fastställas formellt av systemägaren som också ansvarar för att tillföra budgetmedel för säkerhetsåtgärderna.

Av säkerhetsdokumentationen ska framgå:

- Vilka informationskategorier som hanteras i IT-systemet, hur dessa är klassade och vilka som är informationsägare.
- IT-systemets klassningsprofil.
- Sammanfattning och resultat från genomförda gap- och riskanalyser.
- Säkerhetsrelaterade åtgärdsplaner.
- Rutiner för behörighetshantering och loggning.
- Kortfattad beskrivning av rutiner för change management.
- Kortfattad beskrivning av patchningsrutiner.
- Säkerhetsinriktade användarinstruktioner.
- Beskrivning av rutiner för incidenthantering.
- Kontinuitetsplaner.

C5. Kommunikationssäkerhet

Inom Karolinska Institutets verksamhet måste den information som kommuniceras och överförs i KI:s nätverk skyddas så att inte obehöriga kan ta del av den.

När information överförs genom data- eller telekommunikation uppstår risk för obehörig åtkomst och förändring av den överförda informationen. Respektive informationsägare svarar för att analysera behovet av nödvändiga skyddsåtgärder, relaterat till riskerna för obehörig åtkomst eller förändring, samt att dokumentera dessa på lämpligt sätt. Informationsägare ska kommunicera sina behov till KI:s IT-direktör som ansvarar för kravställningen avseende nätverket.

KI:s nätverk ska utformas så att det finns definierade gränssnitt, såväl fysiskt som logiskt, mot andra nätverk. Sammankoppling med andra nätverk får endast ske efter att säkerhetsaspekterna analyserats och nödvändiga skyddsåtgärder vidtagits av respektive nätverks ägare.

Känslig information får aldrig överföras på ett sådant sätt att obehöriga kan ta del av informationen. Detta innebär att överföring via öppna nät i regel måste vara krypterad.

All IT-utrustning som kopplas till KI:s nät ska vara konfigurerad enligt definierad standard och det ska finnas instruktioner för hantering av sådan utrustning. Övriga datorer som behöver kopplas upp mot internet ska separeras från KI:s interna nätverk och ska kopplas via ett så kallat gästnät.

Anvisning för kravställning av kommunikations- och nätverkssäkerhet

Karolinska Institutets IT-direktör ansvarar för övergripande kravställning rörande säkerheten avseende KI:s nätverk och infrastruktur. Nivån på kravställningen ska samordnas med informationssäkerhetsfunktionen samt relevanta informationsägares krav på tillgänglighet och skyddsåtgärder. Denna anvisning ska endast ses som ett stöd avseende vad som ska ingå i kravställningen samt den miniminivå som ska följas inom KI.

Nätverksmiljön

Nätverksmiljön och dess komponenter ska vara dokumenterade och övervakade ur ett säkerhetsperspektiv. Det ska finnas systemskisser över samtliga komponenter som ingår i nätverket och alla anslutningspunkter mot andra nätverk ska vara tydligt utmärkta. Varje komponent ska vara dokumenterad med nätverksnamn, märke, modell, programvara och konfiguration. Det ska även finnas en eller flera logiska systemskisser över samtliga systemsamband.
Tekniska lösningar så som kablage, aktiva nätverkskomponenter och kommunikationsprotokoll ska väljas med utgångspunkt från KI:s krav på informationssäkerhet. Segmentering av nätverk ska användas som en del av den totala säkerhetslösningen för att skydda känslig information och övriga resurser.

Trådlösa nätverk

Då information överförs med hjälp av trådlösa nätverk uppkommer risker, bland annat avseende avlyssning, och därför ska kommunikation över trådlösa nätverk krypteras. Detaljerade instruktioner ska fastställas för design, konfiguration och användning av trådlösa nätverk. Risken för störning av känslig elektronisk utrustning ska alltid beaktas vid användandet av trådlösa nätverk.

Externa nätverk

Anslutning till externa nätverk (utanför KI:s nät) och internet ska regleras genom specifika anvisningar. Internetuppkopplingar och datorer som används av andra än KI:s medarbetare (till exempel gästföreläsare eller besökare) ska vara logiskt separerade från KI:s nät (så kallade gästnät).

Utrustning i nätverket

Det är inte tillåtet att installera eller köra mjukvara som inte är verksamhetsrelaterad på KI:s utrustning som är kopplad mot det interna nätverket. All utrustning (arbetsstationer, bärbara datorer, surfplattor, mobiltelefoner etc.) som ansluts till nätverket ska uppfylla KI:s gällande säkerhetsregler. Användning av programvara på KI:s utrustning får inte ske i strid med gällande upphovsrättslagstiftning. All utrustning som ansluts till KI:s nätverk ska skyddas och vara konfigurerad enligt definierade och dokumenterade standardkonfigurationer. Synkronisering av e-post, kalender etc. får endast ske på utrustning på vilka godkända säkerhetslösningar finns installerade.

Telefoni

Användning av mobiltelefoner ska regleras genom anvisningar avseende användande av e-post och andra interna resurser. Trådlösa telefoner är i regel inte krypterade och lämpar sig därför inte för utbyte av känslig information. Detta gäller till viss del även SMS och taltrafik från mobiltelefon. Vid kommunikation kring känsliga uppgifter över telefon ska det alltid säkerställas att det är rätt person som tar del av uppgifterna.

Informationsöverföring

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om e-post innehållande information med höga skyddskrav avseende konfidentialitet ska sändas till extern part ska lösning med kryptering och signering användas. Avtal som reglerar säker överföring av verksamhetsinformation mellan KI och extern part ska upprättas. Användandet av osäkra klartextprotokoll såsom t.ex. FTP och HTTP ska undvikas och ersättas av säkra alternativ om information med normala eller höga skyddskrav avseende konfidentialitet ska överföras.

C6. Styrning av åtkomst till information

Tillgång till information är viktigt för att kunna bedriva Karolinska Institutets verksamhet. Samtidigt är det viktigt att informationen endast är möjlig att komma åt för de personer som har ett faktiskt och berättigat behov av den. Känslig information måste skyddas från obehörig åtkomst och felaktiga förändringar. Det måste därför säkerställas att tillgång till information endast ges till behöriga personer.

Grundläggande säkerhet

Det är många individer, såväl medarbetare, studenter, uppdragstagare/anknutna, konsulter i verksamheten och till viss del leverantörer, som har åtkomst till KI:s information och system. Därför ska det finnas metoder och rutiner på plats för att kontrollera all åtkomst till information, system, nätverk och tjänster. Åtkomst till information inom KI ska kontrolleras genom nedanstående administrativa och tekniska skyddsåtgärder.

Åtkomstadministration

För att säkerställa att endast behöriga informationsanvändare har tillgång till viss information (både i digital och i fysisk form) ska åtkomsträttigheten godkännas av behörig person/roll innan den tilldelas en användare. Åtkomstens omfattning ska vid varje tillfälle avgränsas till användarens aktuella behov utifrån dennes arbetsuppgifter och organisatoriska tillhörighet. Detaljerade instruktioner avseende hur beställning, registrering, förändring och avregistrering av åtkomsträttigheter ska genomföras, ska definieras och dokumenteras.

Granskning av tilldelade åtkomsträttigheter ska genomföras regelbundet och åtgärder vidtas för att säkerställa att endast vid var tid behöriga användare har åtkomst till respektive informationstillgång och system.

Åtkomstkontroll

Alla användare ska identifieras och verifieras genom användarnamn och lösenord innan de får åtkomst till ett system. För åtkomst till information som informationsklassats till den högsta nivån avseende konfidentialitet krävs stark autentisering i form av tvåfaktorsautentisering. Alla användare ska ha en unik identitet och alla användarkonton ska vara spårbara till en fysisk person.

Loggning och övervakning

För att säkerställa att alla användaraktiviteter är spårbara ska loggning ske på alla verksamhetskritiska IT-system. Detaljerade instruktioner och arbetssätt för uppföljning av loggar och hur eventuella överträdelser ska hanteras ska vara definierade och dokumenterades.

Anvisning för åtkomstadministration

För åtkomst till KI:s nätverk och IT-system ska det finnas detaljerade instruktioner och en organisation för administration av åtkomsträttigheter. Detta för att säkerställa att det endast är godkända åtkomsträttigheter som läggs upp i systemen. Systemägaren eller motsvarande roll för de fall att information inte lagras i ett specifikt IT-system (utan exempelvis i en mappstruktur på gemensam lagringsyta), är ansvarig för instruktion och organisation för respektive system/miljö.

Vid administration av åtkomsträttigheter gäller följande:

- En behovs- och riskanalys ska göras gällande uppsättningen av åtkomsträttigheter i IT-systemet, eller annan elektronisk lagringsyta. Detta för att kunna tilldela rättigheterna på ett korrekt sätt. Analyserna ska genomföras och utvärderas i samråd med informationsägare.
- De åtkomsträttigheter som tilldelas en användare i ett system, eller annan elektronisk lagringsyta, ska inte vara högre än vad som krävs för att denne ska kunna utföra sina aktuella arbetsuppgifter.
- Åtkomsträttigheter till system, eller annan lagringsyta, får endast användas för att utföra de arbetsuppgifter som användaren är ålagd av KI att utföra.
- Om det finns flera ägare till information som behandlas i ett och samma IT-system ska dessa gemensamt komma överens om arbetssätt och instruktioner för åtkomstadministration.
- Användaridentiteter ska vara unika och användas i kombination med personliga lösenord.
- Höga åtkomsträttigheter, s.k. administratörsrättigheter, ska vara personliga och begränsas till så få personer som möjligt. Dessa får endast delas ut efter skriftligt beslut från systemägaren, eller motsvarande roll i de fall information inte lagras i ett specifikt system.
- Höga åtkomsträttigheter, så kallade administratörsrättigheter, för teknisk IT-utrustning ska vara personliga och begränsas till så få användare som möjligt och åtkomster får endast delas ut efter skriftligt beslut från respektive informationsägare.
- För åtkomst till information som klassats till den högsta nivån avseende konfidentialitet krävs tvåfaktorsautentisering.
- Lösenord ska hållas hemliga och följa gällande regelverk för lösenord vid KI[13].

[13] KI:s regler för lösenord: https://ki.se/medarbetare/regler-for-losenord-pa-karolinska-institutet

Instruktioner för åtkomstadministration

Instruktion för kontroll över beställning, förändring och borttagande av åtkomsträttigheter ska fastställas för varje system, eller övrig elektronisk lagringsyta. Instruktionerna ska innehålla minst följande information:

- Hur beställning av tillägg, borttagande och förändring av åtkomsträttigheter ska gå till.
- Vilka mallar eller blanketter som ska fyllas i och hur dessa ska användas.
- Hur de specifika åtkomsträttigheterna som beställs ska specificeras och att konkreta arbetsuppgifter ska kunna kopplas till de olika rättigheterna som beställs.
- Vilka kriterier och arbetsuppgifter användaren ska ha för att ansökan om åtkomsträttighet till IT-systemet, eller annan elektronisk lagringsyta, ska få göras.
- Vem/vilka (roller) som får beställa åtkomsträttigheter.
- Vem/vilka (roller) som beslutar om användaren ska erhålla en åtkomsträttighet.
- Vart beställningen ska skickas samt vem/vilka (roller) som lägger upp åtkomsträttigheten i IT-systemet/annan lagringsyta alternativt beställer rättigheten hos eventuell IT-leverantör.
- Hur leveransen av åtkomsträttigheten och dess tillfälliga lösenord ska ske samt hur det säkerställs att rätt användare erhåller uppgifterna.
- Hur spårbarheten säkerställs, det vill säga hur beställning och godkännande ska sparas och arkiveras.

Anvisning för granskning av åtkomsträttigheter

Befintliga åtkomsträttigheter i Karolinska Institutets IT-system och IT-miljöer ska regelbundet följas upp i syfte att säkerställa att de är förenliga med användarnas behov och arbetsuppgifter och att inte obehöriga har åtkomst till känslig information. Granskningarna ska genomföras med olika frekvens baserat på informationens/IT-systemets informationsklassning enligt följande:

Informationsklass:	**Frekvens:**
K3 och/eller R3	Kvartalsvis
K2 och/eller R2	Kvartalsvis
K1 och/eller R1	Halvårsvis
K0 och/eller R0	Årligen

Behörigheter för särskilda privilegierade åtkomsträttigheter, s.k. administratörsrättigheter, ska alltid granskas minst kvartalsvis. Utöver ovan beskrivna frekvens ska granskningar av alla åtkomsträttigheter även ske vid större organisations- och systemförändringar.

Dokumentation

Då granskningar genomförs är det viktigt att dokumentationen sparas, både för att kunna följa upp hantering kring åtkomsträttigheter men även för att kunna visa för revisorer och annan tillsyns-verksamhet att granskningarna verkligen har genomförts.

Nedanstående punkter ger en vägledning kring vilken typ av dokumentation som ska sparas som ett minimum:

- Underlag (användarlista från IT-systemet) som granskningen baserats på.
- Godkännande/bekräftelse avseende IT-systemets alla tilldelade åtkomsträttigheter.

- Underlag för beställning avseende förändring och borttagande som granskningen genererat.
- Nytt underlag (användarlista från IT-systemet) som visar att förändringar från granskningen har genomförts.

Generell vägledning för granskning av åtkomsträttigheter

OBS! Nedanstående vägledning är generell, förenklad och framtagen för att passa de flesta system, eller annan elektronisk lagringsplats, inom KI. Vägledningen är tänkt som ett stöd vid framtagandet av lokala instruktioner för att säkerställa att regelbunden och ändamålsenlig granskning av åtkomsträttigheter sker.

Regelbundna granskningar av åtkomsträttigheter bör minst innefatta följande aktiviteter:

- Informationsägare eller systemägaren om aktuell arbetsuppgift har blivit delegerad till denne, initierar granskningen genom att be relevant administratör att beställa/ta fram en lista över det aktuella IT-systemets användare och dess åtkomsträttigheter.
- Listan med behörigheter skickas därefter till relevanta chefer, prefekter, administrativa chefer och eventuella andra intressenter (t.ex. informationsägare) vilka således involveras i granskningen genom att de granskar alla konton (både användarkonton och systemkonton) i IT-systemet utifrån följande aspekter:
    - Vem är ägare av kontot?
    - Har den personen behov av ett konto utifrån sina arbetsuppgifter?
    - Är det rätt nivå på åtkomsträttigheter baserat på personens arbetsuppgifter och organisatorisk tillhörighet?
- Administratören av granskningen sammanställer informationen från verksamhetens genomgång och tar därefter fram en förteckning över de förändringar och/eller borttagande av åtkomsträttigheter som ska göras.
- Administratören genomför förändringarna alternativt beställer dem från IT-leverantören.
- Administratören beställer/tar fram en ny lista över IT-systemets åtkomsträttigheter och säkerställer att de beställda förändringarna verkligen har genomförts.
- Administratören slutför granskningen genom att spara den dokumentation som granskningen genererat på därför angiven plats.

Anvisning för loggning och loggranskning

Loggning ska ske på alla IT-system och lagringsplatser (exempelvis då forskningsdata inte lagras i ett specifikt IT-system utan till exempel i en mappstruktur på gemensam lagringsyta) där känslig information lagras. Detta för att säkerställa att relevanta användaraktiviteter och informationssäkerhetshändelser registreras och är spårbara. Informationsägaren ansvarar för att säkerställa att tillfredsställande loggning och loggranskning sker gällande hantering av informationen. Systemägaren, eller motsvarande roll för de fall att information inte lagras i ett specifikt IT-system (utan exempelvis i en mappstruktur på gemensam lagringsyta), ansvarar för att de faktiska granskningarna genomförs.

Loggning

Vid loggning gäller följande:

- Övervakning och loggning ska följa vid var tid gällande relevanta lagkrav. Loggarna ska åtminstone innehålla uppgifter om följande:
    - Samtliga händelser i IT-systemet, eller i annan elektronisk lagringsplats, initierade av en användare eller ett annat system.
    - Vilken användare som initierat händelsen och tidpunkten.
    - Samtliga misslyckade inloggningsförsök i IT-systemet samt vilken IP-adress varifrån inloggningsförsöket gjordes.
    - Systemlarm eller fel.
    - Ändringar, eller försök till ändringar, i IT-systemets säkerhetsuppsättningar och säkerhetsåtgärder.
- Användarna ska informeras om att deras aktiviteter i nätverk och IT-system etc. loggas och i vilket syfte dessa loggar följs upp. Denna information kan exempelvis ges i respektive systems användarinstruktioner eller som automatiskt meddelande i samband med inloggning.
- Samtliga loggfiler ska skyddas mot obehörig åtkomst och manipulation samt omfattas av relevant säkerhetskopiering i enlighet med fastställda instruktioner. Loggar ska sparas i enlighet med vid var tid gällande lagstiftning och informationsägares krav.
- För att säkerställa loggarnas bevisvärde ska loggande systems systemklockor synkroniseras med ett utpekat normalur.

Granskning av loggar

Avseende IT-system som är högt klassade vad avser konfidentialitet (K2 och K3) och riktighet (R2 och R3) ska loggranskning genomföras regelbundet. Granskningarna ska genomföras utifrån fastställda instruktioner enligt följande:

- Instruktionerna ska beskriva vad som loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som betraktas som överträdelse och hur eventuella överträdelser ska hanteras och rapporteras. Beslut om hur ofta loggarna, i sin helhet eller endast vissa delar, ska granskas bör baseras på förekommande risker, där exempelvis värde och känslighet av aktuell information bör övervägas. Systemadministratörers och -operatörers aktiviteter bör dock granskas minst månatligen.
- Om möjligt ska loggarna analyseras med hjälp av automatiserade verktyg. Om detta inte är möjligt ska tillräckliga manuella kontroller i stället utföras.
- Tillgång och åtkomst till logg och logganalysverktyg ska begränsas och regleras med individuell åtkomsttilldelning.
- Underlag från genomförda loggranskningar ska sparas och åtkomst till dessa regleras med individuell åtkomsttilldelning.

C7. Anskaffning, utveckling och underhåll av system

Karolinska Institutets IT-system och den information som hanteras där är av största vikt för verksamheten. För att säkerställa att känslig information hanteras på ett säkert sätt är det viktigt att IT-systemen har rätt funktionella och tekniska förutsättningar. Därför måste säkerhetskraven återspeglas i IT-systemen och hanteras redan vid planeringen av inköp eller utveckling av system.

Grundläggande säkerhet

Att bygga in säkerhet i IT-system samtidigt som de utvecklas är mer kostnadseffektivt och säkert än att tillföra säkerheten efteråt. Inbyggt skydd för personuppgifter är ett krav i GDPR.

I förberedelserna för utveckling eller upphandling av IT-system är det viktigt att säkerställa att informationssäkerhetens olika aspekter konfidentialitet, riktighet, tillgänglighet och spårbarhet beaktas. Detta för att säkerheten ska bli en integrerad del av IT-systemet vilket kräver ett strukturerat tillvägagångssätt och att kraven avseende informationssäkerhet är tydligt definierade. Därför ska en dokumenterad utvecklingsmetod eller ett dokumenterat anskaffningssätt som tar hänsyn till detta användas.

God kunskap om verksamhetens krav (inklusive krav kopplade till informationssäkerhetsaspekterna) är väsentligt om IT-systemet ska kunna uppfylla sitt syfte. Därför ska all systemutveckling och anskaffning av IT-system föregås av en informations- och systemklassning respektive riskanalys.
Utvecklingen eller upphandlingen ska minst beakta följande:

- Tvingande myndighetskrav.
- Interna regler avseende informationssäkerhet.
- Driftstabila och beprövade lösningar.

En strikt och väldefinierad arbetsrutin krävs när nya IT-system eller utvecklade system-komponenter implementeras från utvecklings- och testmiljön in i produktionsmiljön. Vid implementering av nya komponenter eller nya funktioner ska en riskanalys göras. Endast formellt accepterade och godkända IT-system eller systemkomponenter får implementeras i produktionsmiljön.

För att upprätthålla en säker och tillförlitlig tillgång till information ska administration, drift och underhåll av IT-system ske på ett strukturerat och systematiskt sätt enligt en formaliserad och antagen modell för systemförvaltning. Systemägaren för respektive IT-system ansvarar för att ställa krav avseende förvaltningen.

Säkerhetstester bör göras kontinuerligt under utvecklingsprocessen för att i ett tidigt skede upptäcka sårbarheter och brister.

Anvisning för kravställning vid anskaffning och utveckling av system

Vid utveckling eller anskaffning av IT-system ska nedanstående aktiviteter genomföras.

Innan utveckling eller anskaffning

- En informations- och systemklassning ska göras för det berörda IT-systemet.
- En riskanalys ska genomföras för att definiera de informationssäkerhetskrav som ställs på IT-systemet. Dessa krav ska sedan dokumenteras som en del av kravspecifikationen.
- I samband med informationsklassningen ska även en bedömning göras hur den tilltänkta systemlösningen förhåller sig till lagar och förordningar, till exempel GDPR.

Under utveckling eller anskaffning

- Vid utveckling ska vedertagna systemutvecklingsmodeller användas för att säkerställa spårbarheten i utvecklingens alla led.
- Tester ska genomföras i separat testmiljö för att säkerställa riktigheten i IT-systemets utdata. Testdata ska alltid vara anonymiserad och faktiska personuppgifter får aldrig användas i testsammanhang**.** Utdatas riktighet ska utvärderas under testfasen med hjälp av rimlighetskontroller.
- Det ska säkerställas att identifierade säkerhetskrav för IT-systemet implementerats i enlighet med vad som definierats i kravspecifikationen.
- Innan IT-systemet får sättas i produktion ska det genomgå acceptanstest/validering som beställaren ska godkänna.

Produktionssättning av ett utvecklat system

- I beställarens driftgodkännande, som ska ligga till grund för beslut gällande produktionssättning av IT-systemet, ska det ingå en uppföljning över de fördefinierade informationssäkerhetskraven.
- Vid utveckling eller anskaffning ska fullständig system-, användar- och drifts-dokumentation framställas. Driftsdokumentationen ska översiktligt behandla de återstartsrutiner som behövs för IT-systemets avbrottsplanering.
  All dokumentation ska vara färdigställd och tillgänglig för berörda personer senast vid produktionssättning av IT-systemet.

Efter produktionssättning:

- Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. vara skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. Särskilt viktigt är det att genomföra kontroll och granskning av kritiska delar av IT-miljön som direkt eller indirekt stöder IT-system med höga skyddsvärden, samt införande av nya IT-lösningar.
- Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.

Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Revision eller mätning av Karolinska Institutets informationssäkerhet i stort kan även omfatta IT-miljön.

Anvisning för kravställning av systemförvaltning

Systemägaren ansvarar själv, eller genom särskilt utsedd systemförvaltare, för förvaltningen av IT-systemet och de säkerhetskrav som är relaterade till förvaltningen. Systemägaren ansvarar för att åtminstone, men inte uteslutande, nedanstående krav uppfylls inom ramen för förvaltningen av IT-systemet. De inom IT-verksamheten vid KI som arbetar med systemförvaltning behöver likaså ha kunskap om dessa krav.

- Det ska finnas en dokumenterad förvaltningsplan, innehållande instruktioner för administration, drift och underhåll, i syfte att säkerställa att IT-systemet hanteras korrekt utifrån ett informationssäkerhetsperspektiv.

- Det ska finnas aktuell och uppdaterad systemdokumentation vilken ska vara tillgänglig för berörda och behöriga personer vid behov.
- Det ska finnas en avbrottsplan för IT-systemet och planen ska vara kopplad till kontinuitetsplanerna för de verksamhetsområden som IT-systemet stödjer.
- IT-systemets användare ska informeras om IT-systemets skyddsåtgärder och användarna ska erhålla nödvändig säkerhetsutbildning innan de tillåts åtkomst till IT-systemet.
- Alla informationssäkerhetsincidenter som uppdagas inom ramen för förvaltningen ska rapporteras skyndsamt i enlighet med vid var tid gällande anvisningar. För ytterligare information kring incidentrapportering se *Anvisning för rapportering och hantering av informationssäkerhetsincidenter*.
- Alla IT-system ska säkerhetsgranskas kontinuerligt och funktionella fel och brister relaterat till IT-systemet ska kontinuerligt analyseras och rapporteras till systemägaren.
- Då förändringar görs i IT-systemet ska alltid KI:s informationssäkerhetskrav avseende förändringshantering följas.

Systemförvaltaren ska, utöver den praktiska hanteringen av ovanstående ställda krav, bistå systemägaren och informationsansvarige avseende:

- Hanteringen av åtkomstadministration och granskning av åtkomsträttigheter, se *Anvisning Åtkomstadministration* och *Anvisning Granskning av åtkomsträttigheter* för mer information.
- Riskanalyser för IT-systemet samt framtagande av åtgärds- och förbättringsförslag baserade på dessa, se *Anvisning Genomförande av riskanalys* för mer information.

Anvisning för kravställning vid drift utanför Karolinska Institutet

Då KI köper tjänster eller förlägger drift av IT-resurser utanför den egna organisationen ska samma regler avseende informationssäkerhet gälla som när driften hanteras i egen regi. Utöver detta ska även följande regler gälla då drift sker utanför KI:

- Kraven på informationssäkerhet ska definieras baserat på en dokumenterad riskanalys och regleras i avtal parterna emellan. Systemägaren ansvarar för kravställning och uppföljning av dessa krav, men samordning bör ske i de fall leverantören hanterar flera av KI:s IT-resurser.
- Då systemanskaffning, utveckling eller underhåll ingår i den externa partens åtagande ska säkerhetskraven i *Anvisning för kravställning vid anskaffning och utveckling av IT-system* följas.
- Uppföljning av avtalade säkerhetskrav ska ske regelbundet. Detta ska möjliggöras genom att i avtalet specificera att KI har rättighet att genomföra revision och granskning av den tillhandahållna tjänsten och hur väl leverantören uppfyller gällande och relevanta informationssäkerhetskrav.
- Om informationen i IT-systemen innehåller personuppgifter ska parternas roller som personuppgiftsansvarig och personuppgiftsbiträde regleras i avtal. I avtalet ska det specificeras att personuppgiftsbiträdet endast får behandla personuppgifterna i enlighet med instruktioner från den personuppgiftsansvarige. Utöver detta måste

personuppgiftsbiträdet även vidta lämpliga och tillräckliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

- Risker som följer av beroende till en viss leverantör ska minimeras.

Molntjänster

Drift av IT-system som innehåller känslig information, alternativt behöver integreras med andra system, ska inte upphandlas som en molntjänst utan att en noggrann riskanalys först har genomförts och dokumenterats. Utifrån analysens resultat ska nödvändiga åtgärder vidtas och minst följande ska säkerställas:

- Garantier på tillgänglighet ska finnas med i avtalet med leverantören. Tillgängligheten ska motsvara verksamhetens krav.
- Om tillgänglighetskraven är höga ska det finnas en redundant internetförbindelse.
- Avtalet bör innehålla en vitesklausul.
- Avtalet ska specificera vilken eller vilka organisationer som har tillgång till informationen.
- Antalet personer som har tillgång till informationen ska vara begränsat.
- Avtalet ska uttryckligen specificera att leverantören ***inte*** få använda sig av KI:s information för eget eller annan parts bruk utöver vad som specifikt är avtalat.
- Om informationen kommer att hanteras utanför Sverige ska rättsläget vara analyserat och det ska säkerställas att säkerhetskraven för till exempel personuppgifter kan garanteras.
- Exportfunktioner ska finnas i tjänsten så att KI vid avtalsslutet, eller i övrigt vid behov, lätt kan byta leverantör.

Avtalet ska specificera KI:s revisionsmöjligheter så att uppföljning av avtalade säkerhetskrav möjliggörs.

C8. Hantering och rapportering av incidenter

En incident är en händelse som kan få negativ påverkan på Karolinska Institutets verksamhet. Informationssäkerhetsincidenter kan till exempel vara förlust av, eller obehörig åtkomst till, information, stöld av IT-utrustning eller datavirusutbrott m.m. För att minska risken att KI:s verksamhet påverkas vid en incident är det viktigt att alla vet hur man ska agera och vart man ska vända sig för att rapportera avvikande händelser och inträffade informationssäkerhetsincidenter.

IT-verksamheten vid KI har ett ansvar för att kunna stödja i utredningar kring informationssäkerhetsincidenter likväl som att rapportera avvikande aktiviteter i IT-system som skulle kunna klassas som incidenter. En stor del av detta arbete innebär att samla in och analysera loggar. IT-verksamheten är ofta den första linjen som upptäcker incidenter av mer teknisk karaktär, exempelvis dataintrång och skadlig kod. Det är därför viktigt att de som arbetar med IT på KI känner till och kan känna igenom tecken på sådana incidenter.

Likaså ställer detta krav på logghanteringen för det berörda IT-systemet, se mer detaljerad information i kapitel *C5. Styrning av åtkomst till information* under avsnittet *Anvisning för loggning och loggranskning.*

IT-verksamheten ska även agera stödjande och vägledande om en användare är osäker på om en incident har inträffat eller inte.

Vid en inträffad incident av teknisk karaktär behöver KI åtgärda den sårbarheten som har utnyttjats. När sårbarheter kräver tekniska förändringar eller anpassningar är det IT-verksamheten som är ansvariga för att åtgärden hanteras skyndsamt.

Systemspecialister inom KI:s IT-verksamheter kan även behöva bistå vid vissa incidenter där det krävs expertkunskap för att kunna genomföra en utredning och analys av incidenten.

C9. Kontinuitetsplanering

Tillgång till Karolinska Institutets information är en grundförutsättning för att bedriva verksamheten. Vid avbrott i tillgång till information och systemstöd måste det finnas planer och rutiner på plats för att säkerställa att verksamheten trots allt kan fortsätta bedrivas.

Grundläggande säkerhet

Kontinuitetshantering innebär att man i en organisation systematiskt arbetar med att och skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimerar konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar att identifiera kritiska verksamhetsprocesser och dessas beroenden av stöd och resurser som t.ex. personal, lokaler och verktyg. IT-resurser är ofta viktiga stöd för kritiska verksamhetsprocesser som ibland kan vara helt beroende av att det finns tillgängligt och fungerar som avsett. IT-relaterad kontinuitetsplanering är därför en viktig del i informationssäkerhetsarbetet i ambitionen att minimera negativa konsekvenser vid allvarliga incidenter eller avbrott. Syftet är att efter ett större avbrott så snabbt som möjligt återgå till normalläge och att konsekvenserna för verksamheten ska vara så små som möjligt, både under och efter avbrottet. Detta innebär att det för IT-system med höga krav avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott – s.k. avbrottsplaner. Förvaltningsledare ska säkerställa att avbrottsplaner finns på plats och att de motsvarar de krav som finns för systems. Systemens klassning samt identifierade risker påverkar vilka krav som ställs på kontinuitets- och avbrottsplaneringen.

Exempel på säkerhetsåtgärder som är relaterade till kontinuitet är säkerhetskopiering, återläsning av information från säkerhetskopior, fysisk säkerhet och redundans. Lösningarna för att uppnå kontinuitet i verksamheten ska utformas så att de är praktiskt och ekonomiskt genomförbara utifrån vald strategi.

Verksamhetskritiska IT-system ska vid händelse av incidenter och avbrott prioriteras framför IT-system med lägre krav på tillgänglighet.

För IT-system som hanterar känslig information måste det finns dokumenterade avbrottsplaner som är tillgängliga för IT-verksamheten.

Anvisning för kontinuitetsplanering

Kontinuitetsplanering ska ske för KI:s alla institutioner och dess kritiska verksamhetsdelar och dokumenteras i en kontinuitetsplan. Ansvaret för att upprätta kontinuitetsplaner ligger hos informations- och systemägare vid KI däremot kan IT-verksamheten behöva bidra med deras kompetens i vissa delar. Följande områden ska beaktas:

1. **Definition av områden/omfattning och strategi**
   Kontinuitetsplanen ska tydligt ange vilka verksamhetsdelar den täcker och den valda strategin för att återställa dessa. Det kan finnas olika strategier beroende på typ av händelse som får konsekvens för verksamhetsdelens tillgänglighet, samt vilken del planen avser att täcka. Risk- och konsekvensanalyser ska genomföras och bilda grund för den valda strategin.

2. **Risk- och konsekvensanalyser**
   Riskanalyser, som beaktar potentiella sårbarheter och hot för verksamheten och dess nyckeldelar, ska genomföras regelbundet (för mer information se Anvisning Genomförande av riskanalyser). Genom riskanalysarbetet inhämtas information som är nödvändig för att bland annat kunna ta fram en relevant kontinuitetsplan och genomföra förebyggande arbete. I kontinuitetsplaneringen ska riskanalysen även innefatta en konsekvensanalys, där fokus ska ligga på konsekvenserna av bristande tillgänglighet till kritisk information. På så sätt identifieras verksamhetens behov av, och krav på tillgänglighet till, information i syfte att kunna upprätthålla kritiska verksamhetsdelar.

3. **Återställningstider**
   Utifrån resultatet av konsekvensanalysen ska kritiska återstartstider för väsentliga verksamhetsdelar definieras. Fastställande av återstartstider innebär att den maximala tid som aktuell verksamhetsdel tillåts vara otillgänglig ska definieras. Denna tid får i sin tur påverkan på utformningen av de kontinuitetslösningar, åtgärdsaktiviteter och reservrutiner som ska dokumenteras i kontinuitetsplanen.

4. **Kontinuitetslösningar**
   De definierade återställningstiderna utgör underlag för vilka kontinuitetslösningar som ska väljas och hur reservrutinerna ska utformas. Lösningarna för att uppnå kontinuitet i verksamheten ska utformas så att de är praktiskt och ekonomiskt genomförbara utifrån vald strategi. Utformningen av reservrutinerna ska vara så detaljerad att den kan ligga till grund för kontinuitetsplaneringen.

5. **Organisation för att utarbeta, införa och underhålla planen**
   Roller och ansvar för att ta fram och kontinuerligt arbeta med kontinuitetsplanerna ska definieras och kommuniceras. Arbetet med och ansvaret för detta kan med fördel delas upp relaterat till de olika verksamhetsdelar som ska täckas av kontinuitetsplanering. Det är dock viktigt att det finns en utsedd ansvarig person som ansvarar för förvaltning och underhåll av den övergripande kontinuitetsplanen.

6. **Granskning, test och övning**
   Kontinuitetsplaner behöver underhållas, och som en del av detta arbete ingår att planerna regelbundet granskas och uppdateras. Regelbundna övningar av planerna ska också genomföras för att på så sätt testa att de är aktuella, ändamålsenliga och att de verkligen fungerar när de behövs. Dessa övningar fungerar även som utbildning i kontinuitetsplanernas reservrutiner för medarbetare och andra berörda.

Kapitel D: Informationssäkerhet för säkerhetsfunktioner

Målgruppen för kapitlet är främst funktioner inom KI som arbetar med informationssäkerhet, IT-säkerhet och fysisk säkerhet.

Kapitlet innehåller regler och anvisningar för styrning av informationssäkerhet, fysisk säkerhet samt incidenthantering

D1. Samordning av informationssäkerhetsarbetet

KI:s informationssäkerhetsfunktion ansvarar för att samordna informationssäkerhetsarbetet vid KI och att stödja verksamheten. Detta innefattar bland annat:

- att KI:s styrande dokument inom området är aktuella,
- att utveckla och förvalta metoder, vägledningar, hanteringsregler och annat stödmaterial inom informationssäkerhetsområdet,
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom KI, t.ex. genom rådgivning och utbildning,
- att stödja verksamheterna i frågor som rör informationssäkerhet,
- kontroll och uppföljning av informationssäkerheten,
- omvärldsbevakning inom informationssäkerhetsområdet.

D2. Fysisk säkerhet

All information som hanteras i Karolinska Institutets regi måste skyddas fysiskt, oavsett om den finns lagrad digitalt eller om den finns på papper. För att säkerställa att informationen skyddas, oavsett om den hanteras i KI:s egna eller i andras lokaler, är det viktigt att alla tar sitt ansvar för att skydda den fysiskt. KI vill också säkerställa att enbart de personer som har ett faktiskt behov av tillträde till KI:s lokaler får det.

Skyddsnivån på det fysiska skyddet kopplat till informationssäkerhet ska baseras på informationsklassning och genomförda riskanalyser och stå i proportion till de identifierade riskerna. Grundregeln ska vara att känslig information aldrig ska lämnas oskyddad. Utrustning som är känslig, eller behandlar känslig information, ska placeras så att möjligheten till obehörigt tillträde minimeras och utformning av lämpliga skyddsåtgärder underlättas.

IT-utrustning som på något sätt centralt behandlar information ska inrymmas i säkra utrymmen med lämpliga tillträdeskontroller dit endast behöriga personer ges tillträde. Med säkra utrymmen avses utrymmen som är speciellt utformade för att uppfylla högre krav på skal- och brandskydd än ordinarie lokaler, samt har tillgång till kontinuerlig försörjning av el och kyla. För dessa säkra utrymmen ska minst följande säkerhetsåtgärder vara uppfyllda:

- Tillträdeskontroller ska innefatta larm, bemannade receptioner och/eller datoriserade passagekontrollsystem med individuella passerkort och koder.
- Brandskydd, såsom utrymningslarm och släckutrustning, ska finnas i anpassad omfattning. Brännbart material får inte förvaras i säkra utrymmen.
- Klimatanläggning ska finnas för att kompensera för den överskottsvärme som utrustningen alstrar.

Elektronisk utrustning ska skyddas mot elavbrott och andra störningar. Strömförsörjning av verksamhetskritisk utrustning och IT-system ska vara avbrottsfri och ansluten till reservkraft. Tester ska regelbundet genomföras för att säkerställa att övergången till reservkraft fungerar.

Som vägledning för fysisk säkerhet ska MSB:s ”Vägledning för fysisk informationssäkerhet i it-utrymmen” tillämpas[14].

Även information i t.ex. pappersformat och mobila lagringsenheter ska skyddas på lämpligt sätt (i enlighet med hanteringskrav kopplade till informationsklassningen som beslutats för den aktuella informationen).

Skydd av bärbar lagringsmedia och IT-utrustning

Verksamhetsinformation som hanteras utanför KI:s lokaler ska skyddas med anpassade skydds-åtgärder för att motverka risk för förlust av, eller obehörig åtkomst till, information. Detta innefattar bland annat bärbara datorer, mobiltelefoner, USB-minnen, pappersdokument etc.

Lagringsmedia som innehåller känslig information eller licensierade program ska fysiskt förstöras eller skrivas över på ett säkert sätt i samband med avveckling eller återanvändning. Det är inte tillräckligt att använda standardfunktioner för att radera data. (Not: För fysisk säkerhet avseende vanliga lokaler hänvisas till Miljö- & Säkerhetsenhetens regler/instruktioner.)

D3. Hantering och rapportering av incidenter

För att säkerställa att eventuella informationssäkerhetsincidenter får minimal påverkan på KI:s verksamhet ska det finnas en formaliserad process för rapportering och hantering av incidenter. Det ska genom denna process säkerställas att alla incidenter och svagheter relaterade till informationshantering blir rapporterade på ett sådant sätt att lämpliga åtgärder kan vidtas på kort och lång sikt.

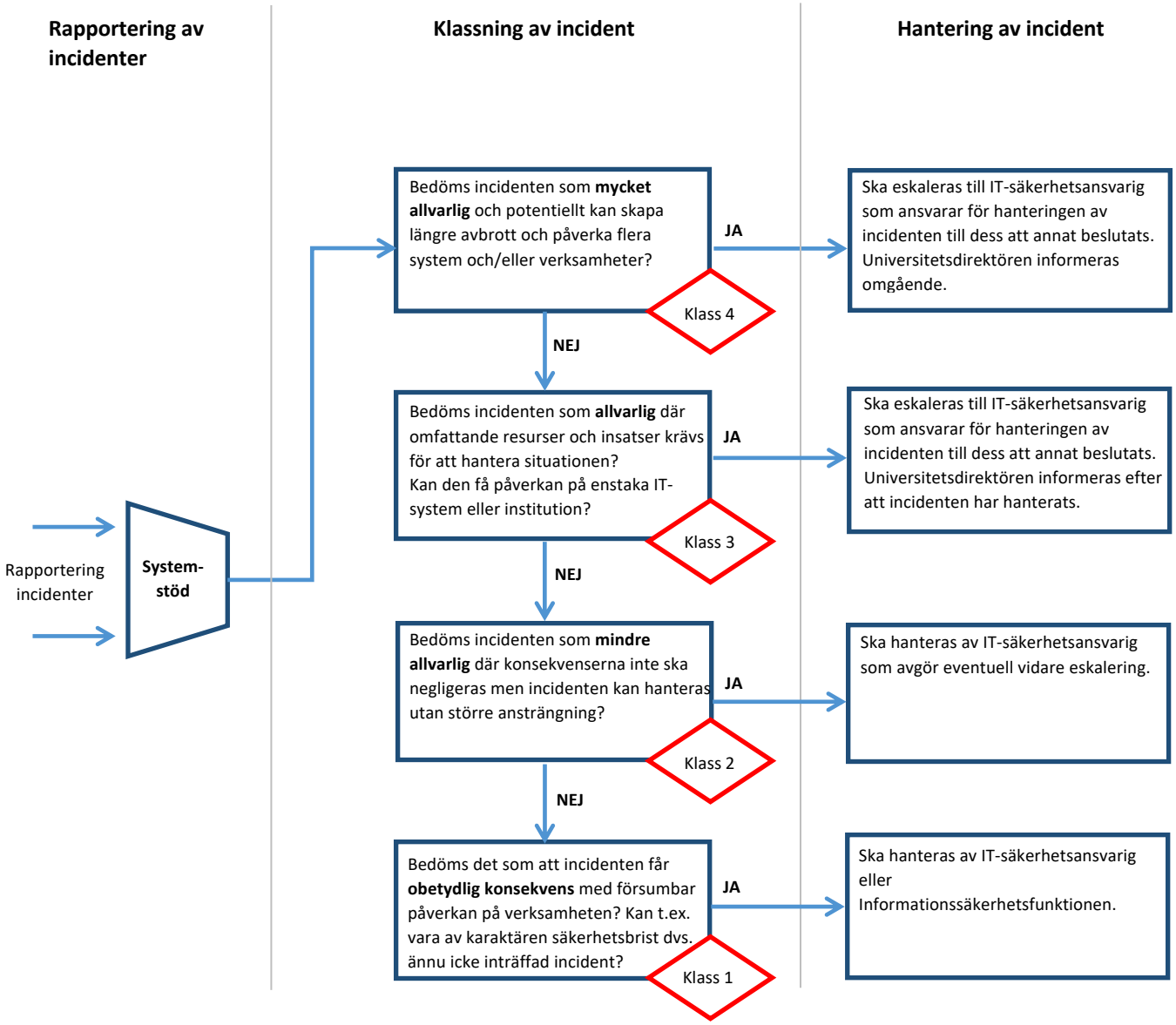
Processen ska säkerställa att incidenter rapporteras till ansvarig myndighet, MSB om allvarlig IT-incident (inom 24 h från upptäckt) eller Datainspektionen om personuppgiftsincident (inom 72 h från upptäckt) i de fall detta erfordras.

Alla inrapporterade incidenter ska efter hantering analyseras med avseende på orsak och påverkan. Detta då det kan finnas ett samband mellan olika incidenter som inte är direkt synligt. Ett antal mindre incidenter kan tillsammans visa på omfattande säkerhetsbrister som är svåra att identifiera utan en genomgående analys. Identifierade säkerhetsbrister definieras som incidenter och ska rapporteras och hanteras enligt ovan.

KI:s IT-säkerhetsansvarige respektive dataskyddsombud hanterar rapportering till tillsynsmyndigheterna varför det är viktigt att incidenter på ”lokal” nivå mycket skyndsamt rapporteras till denna centrala funktion eller KI:s IT-support.

[14] https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

Rapporterade incidenter värderas mot följande fyra klasser:



Hantering av informationssäkerhetsincidenter

IT-säkerhetsansvarig ska (eventuellt i samråd med informationssäkerhetsfunktionen) skyndsamt göra en första analys av incidentens potentiella påverkan för att bedöma hur den ska klassas och om den ska eskaleras vidare i organisationen. Om incidenten innefattar personuppgifter ska även KI:s dataskyddsombud delta i analysen av den potentiella påverkan. IT-säkerhetsansvarig beslutar om prefekten vid berörd verksamhet ska informeras om den rapporterade incidenten.

Rapporterade incidenter ska hanteras i prioritetsordning i relation till den klass som incidenten fått. Hanteringen av incidenter ska omfatta:

- Dokumenterad information om incidenten innehållande; tidpunkt, vad som inträffat, omständigheter, om incidenten innefattar personuppgifter m.m.

- Eventuella bevis ska fastställas genom exempelvis granskning av loggar eller insamling av information från system eller utrustning.
- KI:s IT-avdelning och andra relevanta leverantörer av IT-tjänster ska informeras då detta bedöms nödvändigt. Det ska finnas en formell väg att rapportera incidenter till dessa leverantörer. På samma sätt ska det även finnas en formell väg för leverantörer att rapportera incidenter som inträffat och som påverkar eller riskerar påverka KI. Detta är något som måste skrivas i avtalet med leverantören.
- Vid incident som även har fysisk påverkan ska ansvarig funktion/person för fysisk säkerhet informeras.
- Erfarenhetsåtervinning av hanterade incidenter ska genomföras för att säkerställa en effektiv och ändamålsenlig hantering i framtiden.

Avrapportering informationssäkerhetsincidenter

Avrapportering av incidenter ska göras beroende på klass enligt beskrivning av hantering ovan. Informationssäkerhetsfunktionen och IT-säkerhetsansvarig ska årligen tillse att det skapas en summerande rapport över alla informationssäkerhetsrelaterade incidenter. Dessutom ska det genomföras en analys och ges förslag på eventuella förbättrande åtgärder för att om möjligt undvika liknande incidenter i framtiden. Erfarenheter från incidentrapportering och -hantering bör användas vid genomförande av riskanalyser och som underlag för uppdatering av reglerna för informationssäkerhet.

D4. Efterlevnad och granskning

Informationssäkerheten gällande viktiga verksamhetsprocesser, IT-system och IT-miljön bör regelbundet genomgå oberoende granskningar. Resultatet av dessa granskningar ska avrapporteras till universitetsdirektören och ledningen/konsistoriet. Det ska finnas en tydlig process för hantering av eventuella avvikelser.

Utformningen, driften och användningen av IT-system kan falla under lagstadgade, internt och externt reglerande och avtalsenliga säkerhetskrav. Det åligger varje ansvarig att säkerställa att gällande regler, föreskrifter och lagar efterlevs i verksamheten. Råd gällande specifika rättsliga krav ska sökas från KI:s jurister.

KI:s säkerhetschef är ansvarig för det övergripande ramverket för informationssäkerhet, regler, riktlinjer och anvisningar, vilket årligen ska granskas och vid behov uppdateras inom ramen för det övergripande informationssäkerhetsarbetet. Syftet med detta är att säkerställa att reglerna omfattar eventuella nya legala krav samt nya risker och hot som måste hanteras samt att föreslagna säkerhetslösningar fortfarande är tillräckliga och aktuella. Säkerhetschefen ska årligen sammanställa en rapport till universitetsdirektören avseende arbetet med informationssäkerheten.

Bilaga 1. Informationssäkerhetsorganisation och ansvarsbeskrivningar

Informationssäkerhetsorganisation

Att skydda information på ett lämpligt sätt kräver att informationssäkerhetsarbetet organiseras strukturerat och effektivt. Informationssäkerheten ska vara en naturlig del av det dagliga arbetet. En tydlig organisation för ansvar över och arbete med informationssäkerhet är en förutsättning för att KI ska lyckas i detta arbete.

Grundläggande säkerhet

Universitetsdirektören har fastställt verksamhetens riktlinjer för informationssäkerhet och har inom ramen för sitt uppdrag det yttersta ansvaret för informationssäkerheten inom KI.

Säkerhetschefen har, på uppdrag av universitetsdirektören, till uppgift att säkerställa att det övergripande informationssäkerhetsarbetet bedrivs så effektivt och verksamhetsanpassat som möjligt. Säkerhetschefen verkställer, med stöd av en *samordnare för informationssäkerhet,* samordningen av informationssäkerhetsarbetet inom KI, förvaltar riktlinjer, regler och övergripande anvisningar för informationssäkerhet samt säkerställer att efterlevnaden på verksamhetsnivå följs upp regelbundet och rapporteras till universitetsdirektören. Informationssäkerhetsfunktionen svarar också för stöd till institutionernas arbete med informationssäkerhet samt för koordinering av andra stödåtgärder som kan bli aktuella inom området.

Prefekter inom KI ansvarar för informationssäkerheten inom sitt ansvarsområde som en del i det delegerade verksamhetsansvaret.

Med fördel utser prefekten en *kontaktperson för informationssäkerhet* vid institutionen. De konkreta arbetsuppgifterna för kontaktpersonerna på verksamhetsnivå kan variera mellan olika verksamheter, alltifrån att endast fungera som kontaktperson mot den centrala samordnaren till att stödja prefekten och personalen i det dagliga informationssäkerhetsarbetet. Detta beroende på vilken ansvarsomfattning rollen tilldelas av prefekten. I de fall en kontaktperson inte utses svarar prefekten för kontakterna i frågor som rör informationssäkerhet vid institutionen.

Chefer och *ansvariga* på alla nivåer ska säkerställa att deras medarbetare får tillräcklig utbildning, kontinuerlig information om informationssäkerhet och håller sig till fastställda säkerhetsregler. Prefekten är ansvarig för att det lokalt finns rätt förutsättningar för arbetet med informationssäkerhet och ska regelbundet följa upp och rapportera efterlevnaden inom sitt ansvarsområde till KI:s säkerhetschef.

Alla verksamma på KI, det vill säga medarbetare, studenter, uppdragstagare/anknutna och konsulter i verksamheten, är ansvariga för att skydda verksamhetens information vid hantering av denna. Därför är det viktigt att alla känner till och följer regler och tillhörande anvisningar avseende informationssäkerhet.

KI:s *dataskyddsombud* ska verka för att personuppgifter behandlas i enlighet med GDPR.

Förutom de roller som beskrivits ovan så har även informationsägare, systemägare och IT-direktör ett utpekat ansvar kopplat till KI:s informationssäkerhet. För mer information kring roller och ansvar se *bilaga 2, Ansvarsbeskrivningar* för respektive roll.

Ansvarsbeskrivningar

Universitetsdirektör

Enligt rektors delegation har universitetsdirektören det övergripande ansvaret för KI:s verksamhet i administrativt, rättsligt och ekonomiskt avseende. KI:s universitetsdirektör ansvarar avseende informationssäkerhet för:

- informationssäkerheten på en verksamhetsövergripande nivå samt är ytterst ansvarig för att det finns aktuella och kommunicerade riktlinjer, regler och anvisningar avseende informationssäkerhetsarbetet inom KI.
- det verksamhetsgemensamma arbetet med informationssäkerhet, bland annat inom kontinuitetsplanering, riskhantering och incidenthantering.
- att årligen rapportera kring KI:s informationssäkerhetsarbete till konsistoriet.

Säkerhetschef

KI:s säkerhetschef ansvarar avseende informationssäkerhet för att:

- samordna och koordinera det verksamhetsgemensamma arbetet med informationssäkerhet, bland annat inom kontinuitetsplanering, riskhantering och incidenthantering.
- säkerställa att det övergripande informationssäkerhetsarbetet bedrivs så effektivt och verksamhetsanpassat som möjligt.
- utforma övergripande handlingsplaner samt planera och koordinera informations-säkerhetsarbetet på KI i enlighet med den övergripande informationssäkerhetsprocessen.
- förvalta KI:s ledningssystem för informationssäkerhet och säkerställa att därtill hörande regler och anvisningar hålls aktuella, uppdaterade och kommunicerade.
- ställa krav mot verksamheten avseende informationssäkerhet. Exempelvis avseende övergripande IT-säkerhet och fysisk säkerhet.
- årligen rapportera följande till KI:s universitetsdirektör:
    - Resultat av granskningar avseende skyddsåtgärder som gjorts i enlighet med KI:s regler och anvisningar.
    - Riskanalyser som utförts avseende informationssäkerheten inom KI.
    - Förbättringsåtgärder som vidtagits avseende informationssäkerheten.
    - Summering och analys av de informationssäkerhetsincidenter som inträffat under året.
    - Efterlevnaden av riktlinjer, regler och anvisningar för informationssäkerhet.
- representera KI i relationen till andra myndigheter och verksamheter i informationssäkerhetsfrågor.

Prefekter

Som en del i ansvaret för verksamheten inom respektive institution, som framgår i rektors delegation till prefekter inom KI, ingår övergripande ansvar för informationssäkerheten avseende den information som genereras och hanteras inom institutionen. Prefekten ansvarar för att:

- regelbundet följa upp och rapportera efterlevnaden av informationssäkerhetskrav inom institutionen till KI:s säkerhetschef.

- alla informationstillgångar inom institutionen har utpekade informationssägare samt att tillgångarna informationsklassas. För mer information, se *Informationsklassningsmodell KI*.
- tid och resurser finns avsatta för informationssäkerhetsarbetet inom institutionen.
- institutionsövergripande riskanalyser genomförs regelbundet. För mer information, se *Anvisning Genomförande av riskanalys*.
- kontinuitetsplanering sker och koordineras på institutionsövergripande nivå. För mer information, se *kapitel B9, Anvisning för Kontinuitetsplanering*.
- säkerställa att alla verksamma inom institutionen får tillräcklig utbildning i informationssäkerhet och att de efterlever fastställda informationssäkerhetsregler.
- aktiviteter genomförs för att säkerställa att de verksamma har korrekta åtkomsträttigheter i relation till sin roll/uppgift. Detta genom att följa befintliga instruktioner för tilldelning av åtkomsträttigheter samt att aktivt delta i regelbundna granskningar av åtkomsträttigheter. För mer information, se *Anvisning Åtkomstadministration* och *Anvisning Granskning av åtkomsträttigheter.*
- beakta informationssäkerheten vid rekrytering, anställning och uppsägning. För mer information, se *Anvisning Informationshantering vid rekrytering, anställning och avslut av anställning*.

Informationsägare

Inom Karolinska Institutet ska det finnas utsedda informationsägare vilka ansvarar för att:

- informationen klassas enligt KI:s informationsklassningsmodell. För mer information, se *Informationsklassningsmodell KI*.
- riskanalyser avseende den specifika informationen och därtill hörande informationstillgångar genomförs regelbundet. För mer information, se *Anvisning Genomförande av riskanalys.*
- åtkomsträttigheter för den specifika informationen och därtill hörande informationstillgång är korrekta, att regelbundna granskningar av åtkomsträttigheterna genomförs och att eventuella nödvändiga åtgärder vidtas till följd av resultatet av granskningarna (exempelvis att personer som inte längre ska ha tillgång till informationen i ett visst IT-system tas bort etc.). Arbetet ska genomföras i samarbete med systemägarna för de IT-system som behandlar och tillhandahåller den aktuella informationen. För mer information, se *Anvisning Åtkomstadministration* och *Anvisning Granskning av åtkomsträttigheter.*
- agera kravställare mot relevanta systemägare, det vill säga för alla de IT-system där informationen hanteras, avseende val av skyddsåtgärder för den aktuella informationen.
- loggning och logguppföljning av användaraktiviteter kopplat till informationen genomförs i ändamålsenlig utsträckning. Arbetet ska genomföras i samarbete med systemägarna för de IT-system som behandlar och tillhandahåller informationen. För mer information, se *Anvisning Loggning och loggranskning*.
- personuppgifter hanteras i enlighet med GDPR, vilket exempelvis innebär att hanteringen av personuppgifter ska anmälas till KI:s dataskyddsombud.

- det i enlighet med såväl gällande lagstiftning (Offentlighets- och sekretesslag 2009:400) som KI:s informationsklassningsmodell genomförs en prövning avseende huruvida informationen kan lämnas ut eller inte. Resultatet av prövningen ska dokumenteras och lagras.
- agera kravställare vad avser hur information som lämnas ut till annan part utanför KI ska hanteras.
- besluta om hur informationen får hanteras och förvaras, både i digital och i fysisk form, i det fall att detta avviker från KI:s informationsklassningsmodell. Beslutar informationsansvarige om att informationen får hanteras på sätt som avviker från KI:s informationsklassningsmodell ska detta beslut dokumenteras och lagras. Vid beslut rörande hantering eller förvaring utanför KI ska först en dokumenterad riskanalys genomföras, se *Anvisning Genomförande av riskanalys.*

IT-direktör

KI:s IT-direktör ansvarar inom informationssäkerhetsområdet för:

- att säkerställa efterlevnad avseende de informationssäkerhetskrav som ställs på de system, miljöer och komponenter som IT-avdelningen ansvarar för.
- att utforma detaljerade anvisningar och instruktioner för IT-verksamheten baserat på KI:s regler och anvisningar avseende informationssäkerhet. Anvisningarna ska hållas uppdaterade och följas.
- KI:s IT-infrastruktur och dess säkerhet. För mer information, se *Anvisning Kravställning av kommunikations- och nätverkssäkerhet*.
- att koordinera det övergripande IT-säkerhetsarbetet inom KI.
- att säkerställa att IT-personalen (intern och extern) följer gällande regler för informationssäkerhet.
- att säkerställa att IT-personalen får nödvändig utbildning avseende informationssäkerhet.
- att säkerställa att anlitade leverantörer inom IT-området uppfyller KI:s krav på informationssäkerhet.
- att, i samarbete med respektive systemägare för centrala system, besluta om tilldelning av personliga administratörsrättigheter. För mer information, se *Anvisning Åtkomstadministration*.

Systemägare

KI:s systemägare ansvarar avseende informationssäkerhet för:

- Den övergripande informationssäkerheten avseende det specifika IT-systemet.
- Kravställning avseende IT-systemets driftsäkerhet. För mer information, se *Anvisning Kravställning av driftsäkerhet och service*.
- Att det regelbundet genomförs riskanalyser för IT-systemet. För mer information, se *Anvisning Genomförande av riskanalys*.
- Att definiera och följa upp IT-systemets skyddsåtgärder samt säkerställa att dessa är i enlighet med kraven avseende informationssäkerhet.
- Att upprätta samarbete med informationsägare avseende de informationstillgångar som

hanteras i IT-systemet.

- Att systemförvaltare utses och att kravställning gentemot denne sker avseende informationssäkerhetsarbetet. För mer information, se *Anvisning Kravställning av systemförvaltning.*
- Att säkerställa att kraven avseende systemutveckling och systemförändring följs. För mer information, se *Anvisning Kravställning vid anskaffning och utveckling av IT-system* och *Anvisning Kravställning av driftsäkerhet*.
- Kravställningen av informationssäkerhet och skyddsåtgärder då drift av IT-system sker utanför KI:s verksamhet. För mer information, se *Anvisning Kravställning vid drift utanför Karolinska Institutet*.
- Att det finns en fastställd anvisning och organisation för administration av åtkomsträttigheter till IT-systemet samt att denna används. För mer information, se *Anvisning Åtkomstadministration*.
- Att regelbundna granskningar av åtkomsträttigheter i IT-systemet genomförs samt för att anvisningar finns för hur granskningarna ska genomföras. För mer information, se *Anvisning Granskning av åtkomsträttigheter.*
- Att i samarbete med IT-direktören besluta om och tilldela personliga administratörsrättigheter till centrala system. För mer information, se *Anvisning Åtkomstadministration*.
- Att funktionalitet för loggning finns i IT-systemet i enlighet med de krav som ställs av respektive informationsansvarig för den information som finns i aktuellt system. Ansvarar även för att systemspecifika instruktioner finns för loggranskning av användaraktiviteter i IT-systemet samt för att regelbundna loggranskningar genomförs i enlighet med informationsansvariges krav. För mer information, se *Anvisning Loggning och loggranskning.*

Bilaga 2. Informationssäkerhet för HR- och personalfunktioner

Alla verksamma inom Karolinska Institutet måste förstå sitt ansvar för att skydda KI:s information. Därför behöver alla berörda få löpande information om och utbildning i gällande informationssäkerhetskrav. Detta i syfte att KI kontinuerligt ska kunna bibehålla en lämplig skyddsnivå för informationen.

Det ska säkerställas att alla verksamma förstår sitt ansvar avseende informationssäkerheten inom KI. Syftet är att se till att all information inom KI hanteras enligt gällande regler. Informationssäkerhetsansvaret ska tydliggöras dels vid anställning, dels genom rollbeskrivning. För övriga verksamma ska informationssäkerhetsansvaret tydliggöras i samband med att anknytningsbeslut skrivs och de tilldelas åtkomst till KI:s interna information.

Informationssäkerhetsansvaret inom KI ska vara tydligt definierat. I avsnittet om *Informationssäkerhetsorganisation* i bilaga 1 beskrivs det övergripande ansvaret för informationssäkerhetsarbetet. Det detaljerade informationssäkerhetsansvaret inom KI finns beskrivet i respektive *ansvarsbeskrivning, se bilaga 2*.

Verksamma ska göras medvetna om sitt ansvar avseende informationssäkerheten inom verksamheten. Utöver denna information kan det finnas lokala regler som behöver beaktas.

Samtliga verksamma inom KI ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter i enlighet med fastställda riktlinjer, regler och anvisningar.

Alla som tilldelas åtkomst till KI:s information ska ha fått grundläggande information om gällande regelverk och verksamhetsspecifika krav på informationssäkerhet. Ansvaret för detta ligger på respektive chef. Utbildning och fortbildning inom informationssäkerhet ska vara en kontinuerlig process inom KI.

En viktig typ av information i detta sammanhang är den som handlar om KI:s medarbetare. En korrekt hantering av denna information ska tydliggöras genom anvisningar, rutiner och checklistor inom ramen för personalfunktionens arbete.

Anvisning för informationshantering vid rekrytering, anställning och avslut av anställning

Vid hanteringen av information avseende Karolinska Institutets anställda finns ett flertal moment där informationssäkerheten ska beaktas. Nedan återfinns krav för att säkerställa informationssäkerheten inom respektive delprocess.

Rekrytering

- Den arbetssökandes formella meriter (så som utbildning, diplom, referenser etc.) ska kontrolleras.
- Den arbetssökandes identitet ska kontrolleras för att säkerställa att personen verkligen är den som den utger sig för att vara.
- Vid rekrytering till särskilt känsliga arbetsuppgifter bör ytterligare registerkontroller genomföras av den som rekommenderas för tjänsten.

Anställning och anställningsvillkor

- I samband med anställning ska den anställde informeras om sin skyldighet att uppfylla de krav som ställs i KI:s riktlinjer, regler och anvisningar för informationssäkerhet.

- Alla anställda ska kontinuerligt under anställningstiden göras medvetna om sina skyldigheter enligt punkten ovan samt informeras om gällande regler avseende informationssäkerhet och tillämpliga lagkrav, så som exempelvis GDPR och Offentlighets- och sekretesslagen (2009:400).
- Det ska vara tydligt vilken information som ägs av arbetsgivaren och som inte får förstöras eller kopieras vid avslut av anställningen.
- KI ska i enlighet med kraven i GDPR inte samla in mer information om sina anställda än vad ändamålet kräver.
- Det ska tydliggöras för de anställda att brott mot gällande riktlinjer, regler och anvisningar för informationssäkerhet kan bedömas som misskötsel, vilket är ett brott mot anställningsavtalet, och kan komma att leda till arbetsrättsliga åtgärder.

Avslutande av anställning

- Aktiviteter ska ske för att säkerställa att ansvarsuppgifter överlämnas och att åtkomsträttigheter upphör vid anställningens slut. Det ska även säkerställas att nycklar, tjänstekort och övrig utrustning återlämnas.

Hantering av konsulter och annan extern personal

- Vid anlitande av konsult eller annan extern uppdragstagare ska det klargöras huruvida han eller hon deltar i verksamheten på samma sätt som en anställd och därmed omfattas av offentlighets- och sekretesslagen. I annat fall ska tystnadsplikten regleras civilrättsligt, det vill säga i avtal.
- Om konsult eller annan extern uppdragstagare kan komma att behandla personuppgifter ska KI:s dataskyddsombud kontaktas för att utreda om ett personuppgiftsbiträdesavtal behöver upprättas.
- Konsulter och annan extern personal ska göras medvetna om sina skyldigheter att uppfylla de krav som ställs i KI:s riktlinjer, regler och anvisningar för informationssäkerhet.
- De åtkomsträttigheter (både logiska och fysiska) som tilldelas konsulter och annan extern personal ska följa uppdragstiden. Aktiviteter ska ske för att säkerställa att åtkomsträttigheterna upphör i samband med uppdragets slut.