Riktlinje informationssäkerhet

Skapad: 2018-02-28

Uppdaterad: 2021-06-15

locum.
VÄRDEN FÖR VÅRDEN

VI ÄR EN DEL AV REGION STOCKHOLM

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2018-02-28	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Innehållsförteckning

LOC 2019-0795
Informationssäkerhetsklass: K1

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2018-02-28	Senast ändrat 2021-06-15	Godkänt 2021-06-15

Riktlinje informationssäkerhet

1 Inledning

Varje nämnd, förvaltning, styrelse och bolag inom Region Stockholm ska bedriva ett systematiskt och långsiktigt informationssäkerhetsarbete. Respektive nämnd, styrelse och bolag ansvarar för att det finns ett lokalt ledningssystem för informationssäkerhet inom dess verksamhetsområde.

Locums informationssäkerhetsarbete ska säkerställa att Locums informationstillgångar ges ett skydd som är anpassat till informationens skyddsvärde, föreliggande risk och författningskrav. Informationssäkerhetsarbetet ska bidra till verksamhetens övergripande mål genom att främja kvalitet och effektivitet i arbetet.

För att informationssäkerhetsarbetet inom Locum ska kunna bedrivas systematiskt, kvalitetssäkert och effektivt så ska återkommande risk- och säkerhetsanalyser ligga till grund för löpande omprövning av behovet av skydd för informationstillgångarna.

Informationssäkerhetsarbetet ska även bidra till att upprätthålla förtroendet för Locums förmågaatt hantera skyddsvärd information och värna medborgares rättigheter och personliga integritet.

Locums informationssäkerhetsarbete ska vara uppbyggt så att informationssäkerheten kan upprätthållas även i händelse av kriser eller annan negativ yttre påverkan på verksamheten och bidra till att effekten av sådana händelser begränsas.

En illustration finns på sista sidan i detta dokument.

1.1 Mål och syfte

Målet med riktlinjen är att säkerställa att informationssäkerhetsarbetet inom Locum är tydligt reglerat och att de säkerhetsnivåer som beslutats för verksamheten är kända av alla som hanterar Locums informationstillgångar och därmed har ett ansvar för informationssäkerheten upprätthålls.

Syftet med riktlinjen är att säkerställa att Locums informationstillgångar identifieras, klassificeras och ges en lämplig skyddsnivå med utgångspunkt i att de finns tillgängliga när de behövs (tillgänglighet), att de är korrekta (riktighet), att obehöriga inte kan få tillgång till dem (konfidentialitet) och att händelser i informationsbehandlingen kan spåras (spårbarhet).

1.2 Avgränsningar

Denna riktlinje reglerar informationssäkerhetsarbetet inom Locums verksamhet och de krav som ställs på informationssäkerhet.

Riktlinjen omfattar krav på informationssäkerhet då entreprenörer och leverantörer hanterar Locums informationstillgångar, men ställer inte krav på entreprenörer och leverantörers övriga informationssäkerhetsarbete.

Denna riktlinje baseras på Region Stockholms riktlinjer för informationssäkerhet som gäller för alla nämnder, styrelser och bolag i syfte att medge en enhetlig reglering då information hanteras av flera parter inom regionen.

1.3 Definitioner

Informationssäkerhet
Informationssäkerhet handlar hur informationens konfidentialitet, riktighet och tillgänglighet ska bevaras så att organisationens krav kan uppfyllas.

Informationsbehandlingsresurser
Med informationsbehandlingsresurser avses system, tjänst eller infrastruktur för hantering av information.

Informationstillgångar
Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationsägare
Informationsägaren kravställer informationssäkerheten för en viss informationstillgång och har förståelse för verksamhetens behov av informationssäkerhet.

Systemägare
Systemägare säkerställer att varje system uppfyller de krav på informationssäkerhet som informationsägaren ställt för respektive informationstillgång som hanteras och har förståelse för möjligheten att upprätthålla informationssäkerhet i IT-system.

Systemförvaltare
Systemförvaltaren ansvarar för att varje system uppfyller systemägarens krav, vanligen en medarbetare på IT-enheten.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2018-02-28	Senast ändrat 2021-06-15	Godkänt 2021-06-15

2 Ledning och styrning av informationssäkerheten

2.1 Ledning av informationssäkerhetsarbetet

Locums informationssäkerhetsarbete leds på strategisk nivå av Verkställande direktör (Vd) och ledningsgrupp på uppdrag av styrelsen. Styrelsen ska enligt Region Stockholms riktlinjer för informationssäkerhet informeras om informationssäkerhetsarbetet och vissa beslut ska fattas av styrelsen. I övrigt är ansvaret för informationssäkerheten delegerat till Locums Vd.

På operativ nivå leds informationssäkerhetsarbetet av säkerhetschef som även ansvarar för uppföljning och utvärdering av arbetet. Varje chef och medarbetare har liksom entreprenörer och leverantörer ett delegerat ansvar för att upprätthålla informationssäkerheten inom den egna verksamheten.

Nedan beskrivs hur ansvar och arbetsuppgifter avseende informationssäkerhetsarbetet fördelas på respektive roll inom Locums verksamhet.

2.1.1 Roller och ansvar avseende Locums informationssäkerhetsarbete

Styrelsen

Locums styrelse är ytterst ansvarig för informationssäkerheten inom Locum. Styrelsen ska hållas informerad om informationssäkerhetsarbetet.

Styrelsen är personuppgiftsansvarig för Locum enligt personuppgiftslagen (PuL) . Styrelsen ska därför utse ett eller flera personuppgiftsombud för Locum.

Styrelsens övriga ansvar för informationssäkerhetsarbetet enligt Region Stockholms riktlinjer, såsom att årligen planlägga och löpande följa upp informationssäkerheten, anta styrdokument för informationssäkerheten och vidta åtgärder för att upprätthålla tillräcklig intern kontroll av informationssäkerhetsarbetet, har delegerats till Vd.

Vd

Locums Vd har, på styrelsens uppdrag, ett övergripande ansvar för informations-säkerhetsarbetet. Vd ska vidta åtgärder för att upprätthålla tillräcklig intern kontroll av informationssäkerhetsarbetet och åtminstone årligen rapportera status på informations-säkerheten till styrelsen.

Vd ska anta de styrdokument för informationssäkerhet som krävs inom ramen för Locums ledningssystem, efter beredning av säkerhetschefen. Vd har, inom sin verksamhet, ansvar för att all informationshantering sker i enlighet med Region Stockholms fastställda styrdokument för informationssäkerhet.

Vd ska avsätta resurser för informationssäkerhetsarbetet och utse informationsägare och systemägare för samtliga informationstillgångar och system (i enlighet med den samman-ställning av informationstillgångar som säkerhetschefen ansvarar för och den sammanställning av IT-system som IT-chefen ansvarar för).

Vd ansvarar även för att det sker en kartläggning och en prioritering av vilka verksamheter som är i behov av en kontinuitetsplan samt beslutar i frågor som rör Locums krisorganisation.

Vd:s övriga ansvar för informationssäkerhetsarbetet enligt Region Stockholms riktlinjer, såsom planläggning av informationssäkerhetsarbetet, utformning av lokala styrdokument och upprättande av en förteckning över informationstillgångar samt framtagande av rutiner för rapportering av vidtagna säkerhetsåtgärder och identifierade brister har delegerats till säkerhetschef.

Ledningsgrupp
Locums ledningsgrupp informeras löpande om informationssäkerhetsarbetet i samband med ledningens genomgång (baserat på Locums integrerade och certifierade ledningssystem). Ledningsgruppens medlemmar förmedlar information om informationssäkerhetsarbetet till berörda chefer och medarbetare.

Säkerhetschef
Locums säkerhetschef (som även är Locums säkerhetsskyddschef) samordnar och följer upp informationssäkerhetsarbetet inom Locum och rapporterar till Vd. Säkerhetschef är även utsedd informationssäkerhetssamordnare för Locum och ansvarar därmed för de uppgifter som åligger informationssäkerhetssamordnaren enligt Region Stockholms riktlinjer om informationssäkerhet.

Säkerhetschefen ansvarar för att en förteckning förs över samtliga informationstillgångar inom Locums verksamhet. Förteckningen ska innehålla informationsägare och informations-klassificering för respektive tillgång.

Säkerhetschef ska utforma förslag till lokala styrdokument för informationssäkerhet med utgångspunkt från den egna organisationens specifika behov och ansvarar även för fram-tagande av rutiner för rapportering av incidenter och identifierade brister rörande informationssäkerheten.

Säkerhetschef ska koordinera arbetet avseende genomförande av risk- och säkerhetsanalyser inom Locum och upprätta en handlingsplan för Locums övergripande informationssäkerhets-arbete. Handlingsplanen ska vara utformad med beaktande av regionens övergripande handlingsplan för informationssäkerhet.

Säkerhetschef ska löpande rapportera till ledningen (i samband med ledningens genomgång) vilka analyser av informationssäkerheten som genomförts och vilka säkerhetsåtgärder av större betydelse som vidtagits samt efterlevnaden av Locums styrande dokument avseende informationssäkerhet.

Locums säkerhetschef är kontaktperson mot regionens informationssäkerhetschef och Locums representant i Region Stockholms informationssäkerhetsråd.

Informationssäkerhetsrådet
För att samordna informationssäkerhetsarbetet inom verksamheten har Locum inrättat ett informationssäkerhetsråd. Rådets uppgift är att främja informationssäkerhetsarbetet och identifiera behov av stöd samt föreslå förbättringar, och samordna viktiga informations-säkerhetsaktiviteter.

Informationssäkerhetsrådet består av representanter från säkerhetsenheten och IT-enheten samt digital utveckling. Övriga medarbetare och konsulter kan komma att kallas som föredragande för informationssäkerhetsrådet vid behov.

Säkerhetschef är sammankallande för informationssäkerhetsrådet.

IT-chef
IT-chef leder och samordnar informationssäkerhetsarbetet inom sitt ansvarsområde.

IT-chef upprättar ett register över de IT-system som Locum ansvarar för och deras respektive informationsklassificering samt tillhandahålla de IT-säkerhetslösningar som krävs för att respektive IT-system ska uppfylla kraven enligt gällande informationsklassificering.

IT-chef ansvarar även för att utforma de instruktioner som krävs för att upprätthålla IT-säkerheten inom IT-verksamheten i enlighet med denna riktlinje.

IT-chef säkerställer att personal och leverantörer som anlitas inom IT-verksamheten uppfyller informationssäkerhetskraven för den egna verksamheten och ges tillräcklig utbildning i informationssäkerhetsfrågor.

IT-chef ingår i Locums informationssäkerhetsråd.

Dataskyddsombudet
Locums dataskyddsombud har till uppgift att tillse att personuppgifter behandlas på ett korrekt sätt i enlighet med Dataskyddsförordningen. Dataskyddsombudet ska bland annat kontrollera att bestämmelser och interna styrdokument följs. Dataskyddsombudet är kontaktperson för Datainspektionen som är tillsynsmyndighet när det gäller behandling av personuppgifter. Dataskyddsombudet ska föra en förteckning över de behandlingar av personuppgifter inom sker inom Locum.

Informationsägare
Informationsägare på Locum är Vd och respektive avdelningsdirektör i ledningsgruppen.

Informationsägare utses av Vd och ska säkerställa att respektive informationstillgång klassificeras och ges den informationssäkerhet som krävs för att motsvara klassificeringen.

Varje informationsägare ska klassificera sina respektive informationstillgångar på en övergripande nivå (varje medarbetare ansvarar för klassificering av egna upprättade handlingar). Informationsägaren kravställer genom klassificeringen vilka säkerhetsåtgärder som ska vidtas för att skydda informationen. Klassificeringen ska baseras på genomförda riskanalyser och särskilt ta hänsyn till de konsekvenser som kan uppstå om informations-tillgången skulle bli otillgänglig, eller om informationen röjs för obehöriga. Säkerhetschefen bistår i klassificeringsarbetet och säkerställer att den klassificering som respektive informationsägare genomför resulterar i enhetlig informationssäkerhet för Locums samlade informationstillgångar.

Det ska finnas en utsedd informationsägare för varje informationstillgång som identifierats inom Locums verksamhet. En informationstillgång kan exempelvis utgöras av driftdator, branddator, brandmodeller, förvaltningsmodeller, styrprogram, PTS nivå 2 eller Faciliate (fast. stuktur, inst db).

Om det finns behov av att samordna klassificering av flera informationstillgångar inom en specifik process eller del av verksamheten så kan hantering av dessa tillgångar med fördel samordnas genom att en gemensam informationsägare utses. Det kan exempelvis vara fallet gällande olika typer av fildelningslösningar eller samarbetsplattformar.

När informationstillgångar överförs från Locum till någon annan organisation ska informationsägaren säkerställa att behovet av informationssäkerhet tillgodoses i överföringsprocessen och att Locums informationsklassificering är kommunicerad till mottagaren. Då informationstillgångar överförs till en privat verksamhet ska informationsägaren avtala om informationssäkerhetskrav och hantering med mottagaren (gäller inte vid utlämnande av allmän handling med stöd av offentlighetsprincipen).

Om en informationstillgång omfattar personuppgifter ska informationsägaren anmäla detta till personuppgiftsombudet.

Systemägare
För varje IT-system som Locum ansvarar för finns det en utsedd systemägare. Med IT-system avses såväl verksamhetssystem som system av betydelse för den tekniska infrastrukturen.

Systemägare utses av Vd och ansvarar för att systemet uppfyller de säkerhetskrav som ställs för den information som hanteras i systemet. Det är respektive informationsägares krav som ska ligga till grund för informationssäkerhetsåtgärder. Om en viss informationstillgång ska hanteras av ett IT-system så ska systemet uppfylla de krav på informationssäkerhet som framgår av informationstillgångens klassificering.

Systemägaren ansvarar för att klassificera systemet utifrån vilken informationssäkerhetsklass systemets skyddsnivå uppfyller. Systemägaren ansvarar även för att systemets skyddsnivå specificeras och dokumenteras. Klassificering av samtliga IT-system sammanställs i den systemförteckning som IT-chefen ansvarar för. En systemägare ska utses så snart beslut fattats om anskaffning eller utveckling av ett nytt IT-system som Locum kommer att ansvara för. Systemägaren ska säkerställa att behovet av informationssäkerhet beaktas genom hela anskaffnings-/utvecklingsprocessen.

Systemägaren och informationsägaren ska i samråd med informationssäkerhetssamordnaren, löpande utvärdera systemets säkerhet i förhållande till de informationstillgångar som systemet hanterar och identifiera behov av åtgärder för att anpassa skyddsnivån då förutsättningarna förändras.

Systemförvaltare
Vd utser systemägare för respektive IT-system och vid behov utses en systemförvaltare för systemet. Systemförvaltaren ansvarar för att:

- systemförvaltning och förvaltningsplan upprättas
- driftgodkännande dokumenteras
- avbrottsplan för systemet utarbetas
- användarna informeras om vilken skyddsnivå som gäller för systemet och vilka krav som därmed ställs på dem

- incidenter, funktionsfel och brister rapporteras, dokumenteras, analyseras och hanteras
- instruktioner utformas för beviljande och kontroll av behörigheter till systemet
- rutiner utarbetas för uppföljning av avvikelser eller försök till avvikelser mot åtkomstreglerna
- förteckning förs över vilken information som behandlas av systemet och vem eller vilka som är informationsägare till denna information
- användarna tilldelas behörigheter i enlighet med informationsägarnas beslut
- förteckning över användare och behörigheter förs och regelbundet följs upp
- åtgärder vidtas för att hantera identifierade risker utifrån genomförda riskanalyser
- system- och användardokumentation upprättas och hålls uppdaterad
- användarna ges adekvat utbildning innan de ges åtkomst till IT-systemet

Informationssäkerhetssamordnare
Locums säkerhetschef är informationssäkerhetssamordnare för Locum. För mer information om informationssäkerhetssamordnarens roll och ansvar se beskrivning av säkerhetschefens roll och ansvar ovan.

Enligt Region Stockholms riktlinjer för informationssäkerhet ska det finnas en utsedd informations-säkerhetssamordnare vid Locum. Denne ska vara utsedd av Vd och, oavsett inplacering i organisationen, rapportera direkt till Vd.

Chefer
I enlighet med vad som gäller för övrig verksamhet inom Locum, är ansvaret för informations-säkerheten kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för informationssäkerheten i denna verksamhet.

Utöver informationssäkerhetsansvaret som varje medarbetare har så ansvarar respektive linjechef för informationssäkerhetsåtgärder rörande den egna personalen och uppföljning av informationssäkerheten inom den egna verksamheten.

Vid rekrytering och anställning ansvarar chefen för att, med stöd av HR, säkerställa att:

- Den arbetssökandes identitet verifieras och att formella meriter (såsom utbildning, yrkeslegitimation, referenser etc.) kontrolleras.
- Den arbetssökande informeras om tillåtna bisysslor och vilka slags förhållanden som kan göra en bisyssla otillåten och vilka skyldigheter den arbetssökande har vad gäller att informera Locum om bisysslor.
- Arbetssökande som ska anställas för en säkerhetsklassad befattning, och därmed ska inplaceras i säkerhetsklass, säkerhetsprövas innan beslut om anställning fattas. Detta ingår som en del av HR:s rekryteringsprocess vid bakgrundskontroll.

- Den arbetssökande informeras om sekretessens räckvidd och omfattning och undertecknar ett sekretessbevis där det framgår att den arbetssökande mottagit informationen.

Chefen ska säkerställa att samtliga medarbetare ges tillräcklig utbildning i informationssäkerhetsfrågor för att kunna utföra sina arbetsuppgifter på ett säkert sätt och löpande informeras om gällande regler och de disciplinära åtgärder som medarbetaren kan bli föremål för om reglerna inte efterlevs.

Då en medarbetare avslutar sin anställning ansvarar chefen för att ansvarsuppgifter avlämnas och att åtkomsträttigheter upphör vid anställningens slut samt att nycklar, tjänstekort, handlingar, lagringsmedia och övrig utrustning återlämnas.

Varje chef ska följa upp informationssäkerhetsarbetet inom den egna verksamheten och delta i de uppföljningar som säkerhetsenheten genomför.

Projektområdeschefer
Projektområdeschef ansvarar för informationssäkerheten inom projekt på motsvarande sätt som linjechefer ansvarar för informationssäkerheten inom den egna verksamheten.

Utöver informationssäkerhetsansvaret som varje medarbetare har så ansvarar respektive projektområdeschef för informationssäkerhetsåtgärder rörande projektdeltagare (entreprenörer och leverantörer) och uppföljning av informationssäkerheten inom de projekt som faller inom ansvarsområdet.

Då behov av att tillföra nya projektmedlemmar till ett projekt uppstår ansvarar projektområdeschefen för att säkerställa att:

- Affärsavtal rörande upphandlingar och avrop av tjänster reglerar informationssäkerhetskrav för projektet och projektmedlemmarnas ansvar för hantering av sekretessreglerad information.
- Projektdeltagarens identitet verifieras och att formella meriter (såsom utbildning, yrkeslegitimation, referenser etc.) kontrolleras.
- Projektmedlemmar som ska delta i verksamhet som omfattas av en säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA), och därmed ska inplaceras i säkerhetsklass, säkerhetsprövas innan verksamheten påbörjas.
- Projektmedlemmar informeras om sekretessens räckvidd och omfattning och undertecknar ett sekretessbevis där det framgår att den arbetssökande mottagit informationen.

Projektområdeschefen ska säkerställa att samtliga projektdeltagare ges tillräcklig utbildning i informationssäkerhetsfrågor för att kunna utföra sina arbetsuppgifter på ett säkert sätt och löpande under projektets gång informeras om gällande regler och de disciplinära åtgärder som deltagare kan bli föremål för om reglerna inte efterlevs.

Då en projektdeltagare inte längre ska delta i projektet ansvarar projektområdeschefen för att ansvarsuppgifter avlämnas och att åtkomsträttigheter upphör samt att nycklar, passerkort, handlingar, lagringsmedia och övrig utrustning återlämnas till Locum.

Varje projektområdeschef ska följa upp informationssäkerhetsarbetet inom de projekt som faller inom ansvarsområdet och delta i de uppföljningar som säkerhetsenheten genomför.

Medarbetare
Varje medarbetare har ett eget ansvar för att se till att informationssäkerheten upprätthålls i det dagliga arbetet. Medarbetares ansvar för informationssäkerheten regleras i anställnings-avtalet.

Varje medarbetare har en skyldighet att hålla sig informerad om vilka regler som gäller för informationssäkerheten inom Locums verksamhet och omgående rapportera inträffade informationssäkerhetsincidenter och uppmärksammade brister som kan påverka informations-säkerheten enligt Locums process för incidenthantering.

Entreprenörer och leverantörer
Entreprenörer och leverantörer som deltar i Locums verksamhet har ett ansvar för att upprätthålla informationssäkerheten för den information som de hanterar för Locums räkning. Informationssäkerhetsansvaret för entreprenörer och leverantörer regleras i affärsavtalet och eventuella medföljande bilaga om informationssäkerhet.

Entreprenörer och leverantörer har en skyldighet att hålla sig informerade om vilka regler som gäller för informationssäkerheten inom Locums verksamhet och omgående rapportera inträffade informationssäkerhetsincidenter och uppmärksammade brister som kan påverka informationssäkerheten enligt Locums process för incidenthantering.

Entreprenörer och leverantörer ska särskilt uppmärksamma de förutsättningar rörande offentlighet och sekretess som föreligger inom Locums verksamhet.

2.2 Styrning av informationssäkerheten

Locums informationssäkerhetspolicy (se nedan) och denna riktlinje, med tillhörande bilagor, reglerar informationssäkerheten inom Locums verksamhet.

Locums styrande dokument avseende informationssäkerhet baseras på gällande författnings-krav och Region Stockholms riktlinjer för informationssäkerhet som Locum är skyldiga att följa.

Locums verksamhet är i stor utsträckning processtyrd och regleras i Locums integrerade och certifierade ledningssystem. Styrningen av informationssäkerhetsarbetet ska vara integrerat i ledningssystemet och på sikt är avsikten att Locum ska implementera ett ledningssystem för informationssäkerhet (enligt den internationella standarden ISO/IEC 27001) i det integrerade ledningssystemet.

2.2.1 Locums informationssäkerhetspolicy

Locums policy för IT och informationssäkerhet ska, som ett komplement till aktuell lagstiftning och Region Stockholms styrande dokument och författningssamling, klargöra principer specifika för Locums verksamhet och uppdrag.

Policydokumentet är fastställt av styrelsen och finns publicerat på Locum.se

2.2.2 Informationssäkerhetskrav i avtal med leverantörer och entreprenörer

För att säkerställa att Locums information ges ett enhetligt skydd oavsett i vilken del av verksamheten den hanteras, och av vem, så är det viktigt att entreprenörer och leverantörers ansvar för informationssäkerheten regleras i affärsavtal då tjänster upphandlas eller avropas.

Avtal ska upplysa entreprenörer/leverantörer om att offentlighets- och sekretesslagens bestämmelser är tillämpliga på verksamhet som innebär att de hanterar Locums information inom ramen för uppdrag.

Avtal ska även reglera vilka krav avseende informationssäkerhet som hantering av Locums information ställer på entreprenör/leverantör. Kraven på upprätthållande av informations-säkerhet för Locums information behöver inte enbart gälla sekretessreglerade uppgifter. Då entreprenören/leverantören inte självständigt kan genomföra sekretessgranskningar av Locums information måste informationssäkerheten upprätthållas för all information som ännu inte bedömts som publik/öppen av Locum.

3 Bedömning och hantering av risker

Locums säkerhetsarbete ska bedrivas systematiskt och effektivt och vara anpassat efter verksamhetens behov och förutsättningar. För att åstadkomma detta genomför Locum regelbundet risk- och sårbarhetsanalyser och säkerhetsanalyser på en övergripande nivå.

När det gäller bedömning av risker kopplat till Locums informationstillgångar så genomförs en förenklad riskanalys i samband med informationssäkerhetsklassificering av respektive informationstillgång.

När informationsägare klassificerar en informationstillgång så ska Locums mall för informationsklassificering användas för att dokumentera den riskanalys som ligger till grund för klassificeringsbeslutet.

4 Identifiering och klassificering av informationstillgångar

Inom Locum har informationstillgångarna i IT-system identifierats och klassificerats för respektive informationstillgång. Förteckningen innehåller även uppgifter om informationsägare, systemägare, systemförvaltare.

Locums kriterier för klassificering av informationstillgångar baseras på Region Stockholms riktlinjer för informationssäkerhet och tillhörande tillämpningsanvisningar med undantag för den högsta klassen av konfidentialitet (K4) där Locum enbart klassificerar uppgifter som omfattas av sekretess och som rör Sveriges säkerhet (benämns hemliga uppgifter i säkerhetsskydds-lagstiftningen). Anledningen till detta är att Locum eftersträvar en enkel, överskådlig och enhetlig klassificering som innebär att en viss informationssäkerhetsklassificering alltid innebär en viss hantering av informationen. Då hemliga uppgifter omfattas av krav på säkerhetsskydd och därmed mycket detaljerade hanteringskrav som inte är tillämpliga på andra typer av skyddsvärd information så är det avgörande för efterlevnaden av informationssäkerhetskraven att dessa uppgifter hanteras som en egen konfidentialitetsklass.

I övrigt är det informationstillgångens betydelse för Locums verksamhet eller andra intressenter och konsekvenserna av att informationstillgången röjs, förvanskas, eller görs otillgänglig samt eventuella författningskrav på informationssäkerhet som ska styra vilken informationssäkerhetsklassificering som gäller.

4.1 Bedömning av krav på konfidentialitet

Krav på konfidentialitet innebär att informationen behöver skyddas mot obehörig åtkomst. Vilken konfidentialitetsklass som informationen bedöms tillhöra styrs av vilka konsekvenser som bedöms kunna uppstå om informationen röjs (kommer till obehöriga individers kännedom, se även avsnitt 5 Behörighet). Ju allvarligare konsekvenser, desto högre konfidentialitetsklass.

I tabellen nedan listas de kriterier som gäller för respektive konfidentialitetsklass i samband med informationssäkerhetsklassificering.

Klass	Klassificeringskriterier
K1	Informationstillgång som inte innehåller några uppgifter som omfattas av sekretess,personuppgifter eller andra uppgifter som omfattas av krav på konfidentialitet. Ettspridande av informationen innebär ingen eller försumbar skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av information som publicerats i trycksak eller på internet, eller som avses att publiceras på motsvarande sätt.
K2	Informationstillgång som innehåller uppgifter som omfattas av internt arbetsmaterial, personuppgifter eller andra uppgifter som omfattas av krav på konfidentialitet. Ett spridande av informationen kan innebära måttlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av information som omfattas av internt arbetsmaterial eller personuppgifter.
K3	Informationstillgång som innehåller uppgifter som omfattas av sekretess, personuppgifter eller andra uppgifter som omfattas av höga krav på konfidentialitet. Ett spridande av informationen kan innebära allvarlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av information som omfattas av sekretess till skydd främst för intresset av att förebygga eller beivra brott (18 kap. OSL) eller skyddade personuppgifter.
K4	Informationstillgång som innehåller hemliga uppgifter (uppgifter som omfattas av sekretess och som rör Sveriges säkerhet) och därmed omfattas av mycket höga krav på konfidentialitet. Ett röjande av informationen kan innebära men för Sveriges säkerhet som inte endast är ringa. Kan utgöras av information som omfattas av sekretess till skydd för Sveriges säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer (15 kap. OSL).

4.2 Bedömning av krav på riktighet

Krav på riktighet innebär att informationen behöver skyddas mot obehörig och oavsiktlig förändring eller förvanskning. Vilken riktighetsklass som informationen bedöms tillhöra styrs

av vilka konsekvenser som bedöms kunna uppstå om verksamheten inte längre kan förlita sig på att informationen är korrekt.

I tabellen nedan listas de kriterier som gäller för respektive riktighetsklass i samband med informationssäkerhetsklassificering.

Klass	**Klassificeringskriterier**
R1	Information som inte omfattas av riktighetskrav. Om uppgifterna obehörigen förändras eller verksamheten inte längre kan förlita sig på att informationen inte har förvanskats så kan det innebära ingen eller försumbar skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av referensinformation av mindre betydelse för verksamheten som Locum har tillgång till, men inte ansvarar för.
R2	Information som omfattas av riktighetskrav. Om uppgifterna obehörigen ändras eller om verksamheten inte längre kan förlita sig på att informationen inte har förvanskats så kan det innebära måttlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av information som publicerats på internet eller i sociala medier.
R3	Information som omfattas av höga krav på riktighet. Om uppgifterna obehörigen ändras eller om verksamheten inte längre kan förlita sig på att informationen inte har förvanskats så kan det innebära allvarlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av styrande regelverk, processbeskrivningar och ritningar.
R4	Information som omfattas av mycket höga krav på riktighet. Om uppgifterna obehörigen ändras eller om verksamheten inte längre kan förlita sig på att informationen inte har förvanskats så kan det innebära mycket allvarlig för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av arkivexemplar av affärsavtal, instruktioner för felavhjälpning i driften, loggar från IT-system, krisplaner eller behörigheter för tillgång till IT-system eller fastigheter.

Processägare Direktör affärsstöd	Processledare/Uppdateringsansvarig Säkerhetschef	Kvalitetssamordnare Kvalitetschef	Skapat 2018-02-28	Senast ändrat 2021-06-15	Godkänt 2021-06-15

4.3 Bedömning av krav på tillgänglighet

Krav på tillgänglighet innebär att informationen behöver skyddas mot händelser som kan innebära att informationen görs otillgänglig för behöriga användare. Vilken tillgänglighetsklass som informationen bedöms tillhöra styrs av vilka konsekvenser som bedöms kunna uppstå om informationen inte kan användas i förväntad utsträckning där den behövs och när den behövs.

I tabellen nedan listas de kriterier som gäller för respektive tillgänglighetsklass i samband med informationssäkerhetsklassificering.

Klass	**Klassificeringskriterier**
T1	Information som inte omfattas av tillgänglighetskrav. Om informationen görs otillgänglig för Locums verksamhet under längre perioder så kan det innebära ingen eller försumbar skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av referenslitteratur eller publikationer.
T2	Information som omfattas av tillgänglighetskrav. Om informationen görs otillgänglig för Locums verksamhet under längre perioder så kan det innebära måttlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av styrande dokument, arkiverade handlingar eller publicerad information av strategisk betydelse.
T3	Information som omfattas av höga krav på tillgänglighet. Om informationen görs otillgänglig för Locums verksamhet under kortare perioder så kan det innebära allvarlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av driftinstruktioner, ritningar och fastighetsinformation eller publicerad information av operativ betydelse.
T4	Information som omfattas av mycket höga krav på tillgänglighet. Om informationen görs otillgänglig för Locums verksamhet under kortare perioder så kan det innebära mycket allvarlig skada för Locums verksamhet, annan offentlig eller privat verksamhet, eller enskilda individer. Kan exempelvis utgöras av instruktioner för felavhjälpning i driften eller behörigheter för tillgång till IT-system eller fastigheter.

5 Behörighet

För all information som inte är publik (offentlig) gäller att Locum måste säkerställa att endast behöriga personer får ta del av informationen. Vilka krav som ställs för att en person ska kunna anses vara behörig styrs av informationens konfidentialitetsklass.

Klass	Behörighetskrav
K1	Inga särskilda krav på behörighet ställs för att få ta del av informationen.
K2	För att kunna anses behörig att ta del av information klassificerad som K2 krävs att personen har tillräckliga kunskaper om informationssäkerhet och har tecknat sekretessbevis med Locum samt att personen har behov att ta del av informationen för att kunna utföra sina arbetsuppgifter och är införstådd med att informationen inte får utnyttjas utanför Locums verksamhet.
K3	För att kunna anses behörig att ta del av information klassificerad som K3 krävs att personen har tillräckliga kunskaper om informationssäkerhet och har tecknat sekretessbevis med Locum samt att personen har behov att ta del av informationen för att kunna utföra sina arbetsuppgifter och är införstådd med att informationen inte får utnyttjas utanför Locums verksamhet.
K4	För att kunna anses behörig att ta del av information klassificerad som K4 krävs att personen har genomgått säkerhetsprövning med godkänt resultat, har tecknat sekretessbevis med Locum och har genomgått en grundläggande säkerhetsskydds-utbildning samt att personen har behov av att ta del av informationen för att kunna utföra sina arbetsuppgifter och är införstådd med att informationen inte får utnyttjas utanför Locums verksamhet

5.1 Åtkomst till information

Respektive informationsägare reglerar behörighetskraven för åtkomsten till informations-tillgångar genom informationsklassificeringen. Åtkomst till information ska baseras på behörighetskriterierna ovan. Samtliga beslut om att ge åtkomst till Locums informations-tillgångar ska fattas av informationsägaren och dokumenteras.

All tillgång till elektronisk information inom Locum ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga personer får tillgång till Locums IT-system och informationen i dem. Den som är inloggad i ett IT-system ansvarar för vem som tar del av informationen.

IT-enheten styr och reglerar de behörigheter som kan relateras till IT-system i enlighet med systemägares beslut och instruktioner .

Varje användares identitet ska verifieras genom autentisering. Alla användare ska ha en unik identitet. Det grundläggande kravet på utformningen av identiteter är att de ska vara spårbara till en fysisk person.

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt. Systemadministrativa arbetsuppgifter ska alltid vara kopplade till

personliga användaridentiteter, för att säkerställa spårbarhet avseende genomförda aktiviteter.

Tilldelning av åtkomsträttigheter ska regelbundet följas upp. Detta ska även ske efter varje större organisations- eller systemförändring.

5.2 Behörighetsstyrning för IT-system

Styrning av behörigheter till IT-system hanteras av IT-enheten. IT-enheten beställer rollbaserade behörigheter för Locums personal och entreprenörer/leverantörer. Ansvarig chef (projektområdeschef för entreprenörer/leverantörer) gör, vid behov, tilläggsbeställningar utöver rollbaserade behörigheter.

Varje chef ansvarar för att regelbundet följa upp att medarbetarna ha rätt behörigheter i förhållande till deras arbetsuppgifter. Projektområdeschefer har motsvarande ansvar för uppföljning vad gäller behörigheter som tilldelats entreprenörer/leverantörer.

Informationsägare ansvarar för att på en övergripande nivå regelbundet följa upp tilldelade behörigheter för respektive informationstillgång.

6 Säker hantering av informationstillgångar

En grundläggande förutsättning för att Locums information ska ges ändamålsenlig informationssäkerhet över tid är att informationsklassificeringen ska innebära en enhetlig hantering. Därför är det viktigt att hanteringen av Locums information fungerar på så sätt att en viss klassificering alltid innebär samma hanteringskrav. Detta är en förutsättning för att informationssäkerhetskraven ska vara överskådliga, förutsägbara och upplevas ge avsedd effekt.

6.1 Utformning av handlingar

För upprättade handlingar gäller att handlingar som klassificerats som K1, K2 eller K3 ska följa Locums mallmodell och grafiska profil. I övrigt finns inga informationssäkerhetsrelaterade krav på handlingarnas utformning.

För handlingar innehållande information som klassificerats som K4 gäller att de ska följa Locums mallmodell och den grafiska profil och samt vara försedda med sidnumrering, exemplarnumrering (för varje kopia av handlingen) och en sändlista som anger vem som är den avsedda mottagaren av handlingen.

6.2 Märkning av handlingar och lagringsmedia

Alla handlingar som upprättas inom Locums verksamhet ska märkas med informationens klassificering. Lagringsmedia ska märkas med den högsta informationsklassen som har hanterats (eller som avses hanteras) på respektive lagringsmedium.

Märkning av handlingar och lagringsmedia ska vara utformad i formatet K, R, T (konfidentialitet, riktighet, tillgänglighet) där varje variabel ges ett värde mellan 1 och fyra. En märkning av en handling med höga krav på konfidentialitet, men begränsade krav på

tillgänglighet och riktighet kan till exempel vara K3R2T2. För mer information om klassificering se avsnitt 4.

I vissa fall kan det vara lämpligt att märka en handling som är klassificerad som K3 med en sekretessmarkering för att upplysa om att handlingen omfattas av sekretess. Majoriteten av de handlingar och lagringsmedia som innehåller uppgifter som omfattas av sekretess inom Locums verksamhet kommer dock inte att förses med en sekretessmarkering. Att förse en handling med sekretessmarkering kan exempelvis vara relevant för att upplysa om att sekretess föreligger då sekretessreglerade uppgifter delges till en entreprenör eller leverantör.

Handlingar och lagringsmedia som klassificerats som K4 ska förses med en hemligstämpel. Hemligstämpeln ska omfatta vilket datum som handlingen/ lagringsmediet upprättats och med stöd av vilken paragraf i offentlighets- och sekretesslagen som informationen bedöms omfattas av sekretess och vara av betydelse för Sveriges säkerhet.

6.3 Förvaring av handlingar och lagringsmedia

Nedanstående krav på förvaring av handlingar och lagringsmedia.

- För handlingar och lagringsmedia som innehåller information som klassificerats som K1 finns inga särskilda krav på förvaring.
- Handlingar och lagringsmedia som innehåller information som klassificerats som K3 ska förvaras inlåsta så att inga obehöriga kan komma åt dem.
- Handlingar och lagringsmedia som innehåller information som klassificerats som K4 ska förvaras inlåst i ett säkerhetsskåp godkänt enligt SSF 3492 (tidigare SS3492).
- Observera att det utöver ovanstående krav finns särskilda krav på förvaring av handlingar i arkiv. Dessa krav hanteras av arkivpersonalen med stöd av säkerhetschef.

6.4 Informationssäkerhet vid kontorsarbete

För information som klassificerats som K1 finns inga särskilda krav på informationssäkerhet vid kontorsarbete.

Vid arbete med information som klassificerats som K3 ska den som arbetar med informationen säkerställa att den inte kan röjas för obehöriga personer då den hanteras i kontorsmiljö.

Det är särskilt viktigt att information klassificerad som K3 inte lämnas framme utantillsyn och därför gäller att såväl fysiska som digitala skrivbord ska hållas fria från känslig information (så kallad Clear Desk Policy respektive Clear Screen Policy).

Vid arbete som innebär hantering av information klassificerad som K3 eller högre i kontorsmiljö eller i möteslokaler ska den som bedriver arbetet säkerställa att tillräckligt insynsskydd finns så att informationen inte röjs för obehöriga.

Information som klassificerats som K4 får endast hanteras på arbetsplats och i IT-utrustning som godkänts förändamålet av säkerhetschefen. Ett sådant godkännande ska vara skriftligt.

6.5 Medförande av handlingar och lagringsmedia utanför lokaler

Information som medförs utanför Locums lokaler ska ges ett ändamålsenligt skydd och hanteringsreglerna som framgår av denna riktlinje ska följas oavsett på vilken plats, eller i vilket sammanhang, informationen hanteras.

- För information klassificerad som K1, K2 eller K3 finns inga restriktioner avseende medförande av handlingar och lagringsmedia utanför Locums lokaler.
- För information klassificerad som K4 gäller att medförande utanför Locums lokaler kräver ett skriftligt godkännande av närmaste chef som, innan tillstånd medges, ska samråda med säkerhetschef.
- Förvaring av Locums information i hemmet bör undvikas så långt som möjligt.
- För information klassificerad som K1, K2 eller K3 gäller samma förvaringskrav i hemmet som vid förvaring i Locums lokaler.
- Förvaring i hemmet av information klassificerad som K4 är inte tillåtet.

6.6 Informationssäkerhet vid resor och konferenser

I samband med resor och konferenser är det särskilt viktigt att uppmärksamma behovet av informationssäkerhet.

- Förvaring av information klassificerad som K3 eller K4 i fordon eller på hotellrum i samband med tjänsteresa är inte tillåtet.
- För information klassificerad som K1, K2 eller K3 gäller samma hanteringskrav i samband med resor och konferenser som vid gäller i Locums lokaler.
- Information som klassificerats som K4 får inte behandlas vid konferenser utanför Locums egna lokaler utan skriftligt godkännande från säkerhetschefen.

6.7 Säker distribution av handlingar och lagringsmedia via post

Då handlingar eller lagringsmedia ska distribueras via post ska Locums ordinarie postrutiner följas och endast distributörer som godkänts av Locum får användas.

- För information klassificerad som K1 eller K2 finns inga restriktioner vad gäller distribution via post.
- Då information i digitalt format klassificerad som K3 eller K4 ska distribueras via post ska icke-överskrivningsbara lagringsmedia användas (CD-R, DVD-R). Överskrivningsbara lagringsmedia (CD-RW, DVD-RW eller USB minnen m.m.) som innehåller, eller har innehållit information klassificerad som K3 eller K4 får endast distribueras via post efter skriftligt beslut av säkerhetschefen.
- För information klassificerad som K4 gäller att den endast får distribueras via post om den skickas i ett manipulationsskyddat emballage (säkerhetspåse) som rekommenderat brev genom registraturens försorg.

För vägledning kontakta Locums säkerhetschef.

6.8 Kopiering av handlingar

För information klassificerad som K1 finns inga restriktioner vad gäller kopiering utöver eventuella ekonomiska- eller miljörelaterade krav.

Information som klassificerats som K3 får kopieras på kopiatorer som tillhör Locumoch innehåller hårddiskar som Locum har reglerat äganderätten till.

Information som klassificerats som K4 får inte kopieras på nätverksanslutna kopiatorer. Endast kopiatorer som skriftligen godkänts av säkerhetschefen får användas för ändamålet.

6.9 IT- och kommunikationssäkerhet för användare

6.9.1 Generella krav vid användning av Locums IT-system

Locums information ska som regel bearbetas och lagras med hjälp av IT-system som har tillhandahållits av Locum och så snart det är möjligt sparas på anvisad plats i nätverket. IT-systemens skyddsmekanismer och säkerhetsprogramvaror ska hållas uppdaterade och får inte kringgås eller sättas ur spel.

- Användare får endast installera programvaror eller IT-system som tillhandahålls av Locum eller som godkänts av IT-enheten.
- Användare ska alltid följa gällande lagstiftning, Locums styrdokument, anvisningar och instruktioner.
- Locums IT-resurser (datorer, mobila enheter, nätverk och kringutrustning) är avsedda att användas som arbetsredskap vid tjänsteutövning. Privat användning av till exempel Officepaketet, internet och e-post är tillåten i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga risker eller kostnader för Locum.
- Endast behöriga ska få tillgång till Locums IT-system. Användare ska hantera IT-utrustning på ett sätt som minimerar risken för att obehöriga får tillgång till den, att den stjäls eller går förlorad.
- e-Tjänstekort med PIN-kod ska användas för att säkerställa att användare av IT-system är behöriga. Vid information i lägre skyddsklasser och när det inte är möjligt att använda e-Tjänstekort, ska användaridentitet i kombination med lösenordanvändas.

För att förhindra obehörig åtkomst till IT-system ska användaren inte lämna datorn påloggad. När datorn lämnas ska den låsas. Det ska finnas en funktion som säkerställer automatisk utloggning ur IT-system eller aktivering av lösenordskyddad skärmsläckare efter en viss tids inaktivitet.

6.9.2 Användaridentiteter

Användaridentiteter, lösenord och e-tjänstekort är personliga och får inte lånas ut.

Användare ansvarar för att användaruppgifter (till exempel lösenord) inte blir kända för andra. I de fall användaruppgifter blir kända för andra ansvarar användaren för att lösenordet utan dröjsmål byts i aktuellt IT-system.

Vid misstanke om att ett lösenord kommit i fel händer eller ett e-tjänstekort tappats bort måste det omgående rapporteras så att de kan spärras och bytas ut.

6.9.3 Loggning

För att säkerställa att endast behöriga användare ha tillgång till Locums IT-system så sker loggning av aktiviteten.

Loggar kan kontrolleras som en del i det systematiska arbetet med IT-säkerheten (stickprovs-kontroller) och kan även följas upp på användarnivå på förekommen anledning. IT-enheten reglerar, utifrån verksamhetens behov, i vilken omfattning stickprovskontroller ska förekomma inom Locums verksamhet.

6.9.4 Anslutning av utrustning Locums IT-system

Användare får endast ansluta av Locum tillhandahållen och kontrollerad IT-utrustning till Region Stockholms interna nätverk.

Anslutning av IT-utrustning som inte tillhandahållits av Locum men som krävs för att utföra arbete på uppdrag av verksamheten (som medtas av till exempel konsulter och leverantörer) ska regleras i skriftligt avtal, där det anges vilka säkerhetsåtgärder som ska vidtas för att skydda verksamhetens IT-miljö och informationstillgångar.

IT-utrustning som är ansluten till regionens allmänna nätverk (SLLnet och till SLLnet anslutna LAN) får inte samtidigt vara uppkopplad mot annat nätverk utanför regionens kontroll.

Anställdas anslutning till regionens allmänna nätverk ska vid arbete från annan plats ske genom en kommunikationslösning som är godkänd av regionen (exempelvis via SAM-tjänsten, Säker anslutning till SLLnet).

6.9.5 Lagring av information

Lagring av information får endast ske på interna system eller externa lagringstjänster som godkänts av säkerhetschefen för den informationsklass som informationen bedöms tillhöra.

Av den sammanställning över IT-system och lagringstjänster som IT-enheten upprätthåller framgår vilken informationsklass som får hanteras i respektive system/tjänst.

Känsliga personuppgifter får endast behandlas i externa lagringstjänster som skriftligen godkänts av säkerhetschefen efter samråd med personuppgiftsombudet. Huvudregeln är att det inte är tillåtet att behandla känsliga personuppgifter i externa lagringstjänster om inte särskilda skyddsåtgärder vidtas. Kravet innebär även att användare måste iaktta särskild försiktighet vid användande av till exempel mobiltelefoners funktioner för lagringstjänster.

6.9.6 Privat användning av Locums IT-system

Privat användning av Locums IT-system måste alltid styras av måttfullhet och av den enskildes goda omdöme så att den inte stör verksamheten eller innebär att Locums information utsätts för risk.

Vid privat användning av Region Stockholms IT-system ska användaren alltid följa gällande lagstiftning, Locums riktlinjer och agera i enlighet med Locums värdegrund.

Användande av Locums IT-system och annan utrustning i samband med bisysslor är inte tillåtet.

6.9.7 Användning av internet

En användare ska inte använda Locums IT-system på ett sådant sätt att det finns risk för att Locums anseende skulle kunna skadas (till exempel kunna skadas om en användare besöker olagliga eller olämpliga hemsidor på internet) eller att användningen kränker någon annan person.

Användaren ska agera säkerhetsmedvetet och inte besöka internetsidor som bedöms innebära säkerhetsrisker för regionens IT-miljö, för att undvika skadlig kod (exempelvis virusangrepp) eller onödig belastning av regionens nätverk.

6.9.8 Användning av e-post

Det är endast tillåtet att använda e-postadressen förnamn.efternamn@sll.se eller någon annan e-postadress tillhörande Locum för tjänsteärenden. Privata e-postadresser får inte användas för att behandla Locums information.

Innehavaren av e-postlåda är ansvarig för vad som skickas eller lagras och ska säkerställa att myndighetspost hanteras på ett korrekt sätt. E-post som skickas till eller från Locums e-postadresser eller är lagrad i Locums e-postbrevlådor omfattas av Tryckfrihetsförordningen samt Offentlighets- och sekretesslagen, arkivlagen m.fl. på samma sätt som övriga handlingar.

Varje användare ska utan dröjsmål avgöra om den skickade eller mottagna e-posten utgör allmän handling. E-post som utgör allmän handling ska utan dröjsmål hanteras och registreras i enlighet med gällande regler.

Användaren ska, som grundregel, betrakta e-post som oskyddad. Detta innebär att meddelanden som skickas okrypterat via e-post inte kan betraktas vara skyddade från insyn, och att det därmed finns risk för att andra än den avsedda mottagaren kan ta del av innehållet. Integritetskänsliga personuppgifter som inkommit oskyddade via e-post ska utelämnas ur ett oskyddat e-postsvar eller vidarebefordran, så att de inte sprids vidare i öppna nätverk

Information klassificerad som K1-K2 får distribueras via e-post utan restriktioner.

Information klassificerad som K3 ska skyddas med e-postkrypteringslösning som godkänts av Locums IT-enhet då den skickas internt eller externt i e-postsystemet. Informationen ska i sådana fall inte lagras i e-postsystemet längre tid än nödvändigt.

Distribution av information klassificerad som K4 via e-post är inte tillåtet.

För vägledning kontakta Locums säkerhetschef.

6.9.9 Användning av sociala medier

Information klassificerad som K2, K3 eller K4 får inte kommuniceras i sociala medier.

Det är viktigt att skilja på användning av sociala medier i tjänsten och privat användning av sociala medier. Registrering av Locums e-postadress i sociala medier får endast ske om det ingår i vår verksamhet.

Det är aldrig tillåtet att använda samma lösenord till sociala medier som till regionens interna system.

6.9.10 Telefoni och videokonferens

Information klassificerad som K1 får förmedlas via telefoni eller videokonferens utan restriktioner.

Då uppgifter som klassificerats som K3 förmedlas via telefoni eller videokonferens ska avsändaren försäkra sig om att inga obehöriga kan ta del av samtalet. Endast videokonferenslösningar som skriftligen godkänts av säkerhetschefen får användas för ändamålet. Teams är INTE godkänt för K3.

Behandling av information klassificerad som K4 via telefoni eller videokonferens är inte tillåtet.

6.9.11 SMS, MMS och internetbaserade meddelandetjänster

Information klassificerad som K1 får förmedlas via SMS, MMS eller internetbaserade meddelandetjänster utan restriktioner så länge kraven på registrering av allmänna handlingar efterlevs.

Information klassificerad som K2 får förmedlas via SMS, MMS eller internetbaserade meddelandetjänster som skriftligen godkänts av säkerhetschefen så länge kraven på registrering av allmänna handlingar efterlevs.

Behandling av information klassificerad som K3 eller K4 via SMS, MMS och internetbaserade meddelandetjänster är inte tillåtet.

6.9.12 Telefax

Information klassificerad som K1 får skickas via fax utan restriktioner.

Om information klassificerad som K2 eller K3 skickas via fax så ansvarar avsändaren för att säkerställa att rätt mottagare tar emot informationen och att informationen inte röjs till någon obehörig.

Överföring av information klassificerad som K4 via fax är inte tillåtet med undantag för fax som innehåller ett av Försvarsmakten godkänt krypto (s.k. kryfax). Kryfax finns att tillgå genom säkerhetschefens försorg.

6.9.13 Utskrifter

Information klassificerad som K1 får skrivas ut utan restriktioner.

För information klassificerad som K2 eller K3 gäller att informationen får skrivas ut på skrivare som tillhör Locum och innehåller hårddiskar som Locum har reglerat äganderätten till. Utskrifter får inte lämnas obevakade och s.k. Follow Me-printing eller Pull Print ska användas där det finns tillgängligt.

Information som klassificerats som K4 får inte skrivas ut på nätverksanslutna skrivare. Endast skrivare som skriftligen godkänts av säkerhetschefen får användas för ändamålet.

6.9.14 Återanvändning av IT-utrustning och lagringsmedia

Återanvändning innebär, i det här sammanhanget, att IT-utrustning eller lagringsmedia som inte längre behövs för det ändamål som den anskaffats används för andra ändamål.

IT-utrustning och lagringsmedia som innehåller, eller har innehållit, information klassificerad som K1 får återanvändas inom Locums verksamhet utan restriktioner.

IT-utrustning och lagringsmedia som innehåller, eller har innehållit, information klassificerad som K2 eller K3 får återanvändas inom Locums verksamhet efter formatering och överskrivning genom IT-enhetens försorg med överskrivningsverktyg som godkänts av säkerhetschefen.

IT-utrustning och lagringsmedia som innehåller, eller har innehållit, information klassificerad som K4 får inte återanvändas.

6.9.15 Användaridentiteter, lösenord och e-tjänstekort

Alla användaridentiteter, lösenord, e-tjänstekort och behörigheter är personliga och ska skyddas mot obehörig åtkomst. De ska kvitteras då de mottas av användaren och kunna visas upp på anmodan av säkerhetschefen.

6.10 Arkiv och register

6.10.1 Registrering och kvittens av handlingar och lagringsmedia

Alla inkomna och upprättade handlingar inom Locums verksamhet ska som regel registreras i diariet så snart de har inkommit eller upprättats.

Det finns inga särskilda krav på registrering och kvittens för handlingar och lagringsmedia klassificerade som K1, K2 eller K3.

För handlingar och lagringsmedia klassificerade som K4 gäller att samtliga handlingar och samtliga lagringsmedia ska registreras och kvitteras genom registraturens försorg.

6.10.2 Inventering

För informationstillgångar klassificerade som K1, K2 eller K3 finns inga krav på regelbunden inventering av handlingar eller lagringsmedia. Inventering kan dock ske vid behov på anmodan från säkerhetschefen.

Handlingar och lagringsmedia klassificerade som K4 ska inventeras årligen genom registraturens försorg. Den som har handlingarna i sin vård ska bistå vid inventeringen.

6.10.3 Återlämnande av handlingar och lagringsmedia

För handlingar och lagringsmedia som innehåller, eller har innehållit, information klassificerad som K1 finns inga krav på återlämnande utöver de allmänna kraven på återlämnande av IT-utrustning som tillhör Locum i samband med avslutande av tjänst.

För handlingar klassificerade som K2 gäller att de ska lämnas för återvinning i ett av Locum tillhandahållet kärl för pappersåtervinning.

För handlingar klassificerade som K3 gäller att de ska lämnas för återvinning i ett förslutet sekretesskärl.

All lagringsmedia ska återlämnas till IT för överskrivning eller destruktion då de inte längre behövs i verksamheten.

6.10.4 Destruktion av handlingar och lagringsmedia

För handlingar och lagringsmedia som innehåller, eller har innehållit, information klassificerad som K1 eller K2 finns inga krav på destruktion.

- Destruktion av handlingar klassificerade som K3 sker genom leverantörs försorg. Handlingarna ska lämnas för återvinning i ett förslutet sekretess-kärl.
- All destruktion av lagringsmedia sker genom mekanisk destruktion eller avmagnetisering genom IT-enhetens försorg.
- Destruktion av handlingar klassificerade som K4 sker genom att de tuggas i en destruktör med maximal spånstorlek 1.2 x 15 mm alternativt 2x2 mm.
- Observera att destruktion av en handling endast får ske om handlingen ska gallras då den inte ska arkiveras enligt gällande arkivföreskrifter.
- Med gallring i offentlig verksamhet menas avsiktlig och kontrollerad förstöring av allmänna handlingar. Beslutanderätten om gallring är inom Region Stockholm delegerad till Regionarkivet genom Dokument- och arkivreglementet. Alla regionens verksamheter ska ha en bevarande och gallringsplan. För journalhantering finns särskilda bestämmelser. Vägledning för hur bevarande, rensning och gallring ska ske inom regionen finns hos Regionarkivet.
- Allmänna handlingar som finns i offentlig verksamhet får enbart gallras enligt regionarkivets beslutade bevarande- och gallringsplaner, eller efter särskilt beslut av regionarkivet. Detta gäller oavsett i vilket medium handlingen finns lagrad.
- Handlingar som finns inom offentlig verksamhet och som inte är allmänna kan rensas vid behov. Varje handläggare är ansvarig för att avgöra vilka handlingar som kan rensas och vilka som är allmänna i enlighet med de regler som finns och oavsett i vilket medium handlingen finns lagrat.

6.10.5 Sekretessgranskning och utlämnande av allmänna handlingar

En begäran om utlämnande av en allmän handling med stöd av offentlighetsprincipen ska alltid hanteras skyndsamt och korrekt med bibehållet sekretesskydd. En begäran att få del av kopior av allmän handling ska hanteras inom en eller några dagar beroende på den arbetsinsats som erfordras. En begäran att få läsa en allmän handling på plats hos myndigheten ska hanteras omgående.

En begäran att ta del av handling som inkommer i skrift (via post eller e-post) ska diarieföras. Om begäran inkommer via telefon skall tjänsteanteckning upprättas och diarieföras, för att det i efterhand skall gå att återfinna datum för begäran liksom begärans innehåll.

Om en anställd inom Locum, har ansvar för en handling, är det i första hand den anställde som ska pröva om handlingen ska lämnas ut.

Ett ärende avseende begäran att få ut handlingar läggs upp och handläggare tillsätts enligt följande:

- Om begäran avser pågående ärenden utses aktuell handläggare till handläggare av inkommen begäran
- Om begäran avser avslutade ärenden utses registrator till handläggare av inkommen begäran
- Om begäran avser handlingar som inte tillhör något ärende kontaktas (chefen för registraturen) för utseende av handläggare
- Förfrågningar från journalister hanteras av pressansvarig.

Om handläggaren bedömer att det inte föreligger någon grund för sekretess så ska handlingen utlämnas i sin helhet.

Vid bedömning av sekretessgrund ska även informationens omfattning beaktas då en aggregerad mängd information som i sina beståndsdelar inte är skyddsvärd kan omfattas av sekretess om man av helheten kan utläsa uppgifter som är sekretessreglerade.

Om handläggaren bedömer att den begärda handlingen inte kan lämnas ut, endast delvis kan lämnas ut eller endast kan lämnas ut med förbehåll som reglerar hur mottagaren får använda sig av informationen i handlingen så ska ett motiverat beslut fattas och delges den som begärt ut handlingen.

Ett sådant beslut ska innehålla en hänvisning till aktuell bestämmelse i offentlighets- och sekretesslagen (2009:400) och av beslutet ska framgå, utöver att sökanden kommer att nekas tillgång till information, också att han/hon kan begära ett s.k. myndighetsbeslut (d.v.s. ett beslut från Locum AB) på att handlingen inte kommer att lämnas ut helt eller delvis.

Den person som begärt utlämnandet ska även underrättas om att han/hon behöver myndighetsbeslutet för att kunna överklaga myndighetens nekande om utlämnande till högre instans. Myndighetsbeslutet fattas av Vd, enligt delegation i den av styrelsen beslutade Vd-instruktionen. Vd har, med stöd av Vd-instruktionen, lämnat fullmakt till ekonomidirektören och bolagsjurist att fatta sådant myndighetsbeslut.

Gör myndigheten samma bedömning som handläggaren och nekar att lämna ut handlingen kan sökanden med myndighetsbeslutet som grund överklaga till kammarrätten. Gör kammarrätten samma bedömning så är nästa instans regeringsrätten.

I samband med sekretessgranskning av begärda handlingar så är det särskilt viktigt att uppmärksamma att Locum inte får efterforska vem som begärt ut en handling, eller i vilket syfte handlingen har begärts ut, i större utsträckning än som behövs för att myndigheten skall kunna pröva om hinder föreligger mot att handlingen lämnas ut.

Då den sekretessgrund som identifierats innebär ett rakt skaderekvisit (d.v.s. att uppgifterna i handlingen som huvudregel är offentliga) så får identitet och syfte inte efterforskas.

Om sekretessgrunden innebär ett omvänt skaderekvisit (d.v.s. att uppgifterna i handlingen som huvudregel är sekretessbelagda och för att uppgifterna ska kunna lämnas ut måste det stå klart att utlämnandet inte kan anses leda till skada) kan handläggaren däremot vara skyldig att

efterforska identitet och/eller syfte med begäran för att kunna säkerställa att ett utlämnande kan ske utan att skada uppstår.

Vid oklarheter om skäl för sekretess föreligger eller hur beslut skall utformas kontaktas bolagsjurist.

7 Utbildning och information avseende informationssäkerhet

En grundförutsättning för att informationssäkerhetsarbetet ska få avsedd effekt är att de personer som hanterar Locums information har tillräckliga kunskaper om informationssäkerhet för att kunna utföra sina arbetsuppgifter på ett säkert sätt.

För att policys, riktlinjer och vägledningar ska nå ut till de som omfattas av informationssäkerhetskraven så är det avgörande att medarbetare, chefer, entreprenörer och leverantörer genomgår informationssäkerhetsutbildning i den omfattning som krävs baserat på arbetsuppgifter och ansvar för informationssäkerhetsfrågor.

7.1 Datorstödd informationssäkerhetsutbildning för användare (DISA)

Samtliga medarbetare och chefer inom Locum ska genomföra den datorstödda informationssäkerhetsutbildning för användare (DISA) som Region Stockholm tillhandahåller. Informationssäkerhet ska vara en del av introduktionsutbildningen för nyanställda.

Utbildningen ska genomföras i samband med att personen påbörjar sin anställning och repeteras vart tredje år.

Även entreprenörer och leverantörer ska åläggas att genomföra DISA, eller motsvarande informationssäkerhetsutbildning, innan deltagande i Locums verksamhet påbörjas.

7.2 Målgruppsanpassad informationssäkerhetsutbildning

För de personer som har ett särskilt informationssäkerhetsansvar, eller som av andra skäl behöver det, tillhandahålls målgruppsanpassad informationssäkerhetsutbildning.

Det kan till exempel vara relevant för lokala säkerhetssamordnare, registratorer, arkivarier och chefer på olika nivåer att genomgå informationssäkerhetsutbildningar som specifikt fokuserar på deras ansvar och vad de förväntas göra inom ramen för sin nyckelroll i Locums övergripande informationssäkerhetsarbete.

Vilka målgruppsanpassade informationssäkerhetsutbildningar som erbjuds fastställs årligen i Locums utbildningsplan som HR ansvarar för i samråd med säkerhetsenheten.

7.3 Möjlighet till fortbildning inom informationssäkerhet

Locum uppmuntrar personer som har ett särskilt informationssäkerhetsansvar att fortbilda sig inom informationssäkerhetsområdet.

Möjligheter till fortbildning kan bland annat erbjudas inom regionen eller genom samarbete med andra myndigheter i stockholmregionen.

7.3.1 Dokumentation av genomförda informationssäkerhetsutbildningar

Allt deltagande i informationssäkerhetsutbildningar ska dokumenteras och registreras i Locums system för utbildningsuppföljning. Säkerhetsenheten följer årligen upp deltagandet i säkerhetsutbildningar på en övergripande nivå.

8 Kontinuitetsplanering i informationssäkerhetsarbetet

Kontinuitetsplanering i informationssäkerhetsarbetet syftar både till att upprätthålla tillgänglighet till information baserat på informationens klassificering och att upprätthålla informationssäkerhetsfunktioner under olika förhållanden.

Målet med kontinuitetsplaneringen är att Locum ska kunna upprätthålla kritiska verksamheter, på rimlig nivå, vid olika typer störningar. För att fastställa vad som utgör en rimlig nivå är det viktigt att det för samtliga verksamheter och IT-system finns fastställda nivåer för hur länge ett stillestånd kan accepteras.

Informationssäkerhet ska vara en integrerad del i Locums kontinuitetsarbete. Processer och rutiner för krisberedskap ska inkludera hantering av informationssäkerhetsincidenter. I verksamhetens kontinuitetsplan ska det behandlas hur verksamheten ska bedrivas vid avsaknad av kritiska funktioner, informationstillgångar och IT-system samt hur återgång till normalläge ska ske.

Kontinuitetsplaner och återstartsplaner skall finnas för all information och alla system som klassats i tillgänglighetsklass T2. Det ska finnas fastställda och aktuella reservrutiner för katastrofsituationer, störningar eller oplanerade avbrott. Rutinerna kan vara såväl manuella som IT-baserade.

Kontinuitetsplanerna ska testas regelbundet, minst årligen, enligt fastställd plan samt efter större organisationsförändringar. Planerna ska underhållas genom regelbundna granskningar och övningar, för att säkerställa att de är aktuella och ändamålsenliga.

9 Hantering av informationssäkerhetsincidenter

Medarbetare, entreprenörer och leverantörer är skyldiga att omgående rapportera inträffade informationssäkerhetsincidenter och identifierade informationssäkerhetsbrister i enlighet med Locums process för incidenthantering.

9.1 Incidentrapportering via Locum.se

Informationssäkerhetsincidenter anmäls av medarbetare i incidenthanteringssystemet Reqs, och behandlas därefter av Säkerhetsavdelningen.

IT-säkerhetsincidenter anmäls till IT helpdesk, men incidenter av allvarligare karaktär registreras även i systemet för incidenthantering (Reqs).

För mer information se Locums process för incidenthantering på intranätet.

Akuta IT-incidenter som kräver omedelbara åtgärder (exempelvis förlust av IT-utrustning eller förekomst av skadlig kod i form av virus, trojaner el dyl.) ska även rapporteras direkt till IT-driftorganisationen, via supporten.

Mottagare av en incidentrapport som rör en informationssäkerhetsincident ska bedöma vilken skada som eventuellt har uppstått och vilka åtgärder som kan vidtas på kort och lång sikt för att minimera risken för ytterligare skada för verksamheten. Denna bedömning ska, så snart som möjligt, dokumenteras och delges säkerhetschefen.

Vid hantering och utredning av en inträffad informationssäkerhetsincident ska särskild försiktighet iakttas för att undvika att försvåra en eventuell brottsutredning genom att påverka bevismaterial.

10 Uppföljning och utvärdering av informationssäkerheten

Locums informationssäkerhetsarbete ska löpande följas upp och utvärderas för att säkerställa att informationen ges ett effektivt och ändamålsenligt skydd i alla delar av verksamheten och att samtliga krav på Locums informationssäkerhet är uppfyllda.

10.1 Egenkontroll

Varje chef ska kontrollera att denna riktlinje efterlevs och att informationssäkerheten upprätthålls inom den egna verksamheten.

Alla medarbetare, entreprenörer och leverantörer ska löpande säkerställa att det dagliga arbetet bedrivs på ett säkert sätt och att eventuella brister i informationssäkerheten uppmärksammas.

10.2 Kontroller och granskningar

Säkerhetschef ansvarar för att säkerhetsarbetet följs upp och utvärderas på en övergripande nivå och att resultatet av genomförda kontroller återkopplas till ledningen i samband med ledningens genomgång.

Säkerhetsenheten genomför föranmälda kontroller av informationssäkerhetsarbetet för Locums olika verksamheter. Kontroller genomförs så långt som möjligt i samråd med berörd verksamhet. Om det finns anledning att anta att informationssäkerheten brister trots påpekanden kan oanmälda kontroller komma att genomföras.

Granskningar av informationssäkerheten kan även initieras av Region Stockholms informationssäkerhetsorganisation eller av regionens revisorer; på eget initiativ eller inom ramen för en planerad revision.

Medarbetares användning av regionens IT-system kan komma att följas upp vid misstanke om brott mot gällande författning eller regionens styrande regelverk. Inom Locum beslutar säkerhetschefen, efter dialog med HR, om kontroll av medarbetares användning ska ske (t.ex. med hjälp av analys av systemloggar) och om några åtgärder ska vidtas i det enskilda fallet i samband med överträdelser. Kontrollen avser i sådana fall en specifik individ. Kontroll kan även avse trafiken i lokala nätverk.

IT-chef ansvarar för att regelbundna kontroller av informationssäkerheten kring Locums IT-system genomförs. Kontrollerna ska omfatta hur systemen förhåller sig till gällande författning och riktlinjer.

Alla kontroller av informationssäkerheten inom Locums verksamhet ska dokumenteras och en kopia av dokumentationen ska delges säkerhetschefen.

10.3 Dokumentation

Alla genomförda säkerhetskontroller ska dokumenteras och dokumentationen förvaras hos säkerhetsenheten. Observera att dokumentation avseende genomförda säkerhetskontroller kan innehålla uppgifter om ännu inte åtgärdade brister i informations-säkerhetsarbetet och därmed vara mycket känsliga.

10.4 Utvärdering och återkoppling till ansvariga

Enligt Region Stockholms riktlinjer för informationssäkerhet är Locums styrelse ytterst ansvarig för informationssäkerheten och det åligger styrelsen att löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Med utvärdering av informationssäkerhetsarbetet avses såväl efterlevnad av Locums styrande dokument avseende informationssäkerhet (främst denna riktlinje) som utvärdering av huruvida de styrande dokumenten har avsedd effekt.

Locums säkerhetschef återkopplar resultatet av genomförda kontroller och utvärderingar till ledningsgruppen, som i sin tur ansvarar för att informera styrelsen. Eventuella identifierade brister av väsentlig karaktär rapporteras av säkerhetschefen till regionens informations-säkerhetschef.

11 Disciplinära åtgärder

Misskötsel eller bristande efterlevnad av gällande lagstiftning eller Locums riktlinjer kan komma att resultera i disciplinära åtgärder.

Disciplinära åtgärder för medarbetare regleras i anställningsavtal.

Disciplinära åtgärder för leverantörer och entreprenörer regleras i affärsavtal samt, i förekommande fall, i särskild bilaga till affärsavtalet.

Medarbetares tillgång till Locums IT-system kan stängas av vid misstanke om brott mot gällande författning eller Locums riktlinjer. Avstängning kan också ske om användningen bedöms utgöra en allvarlig risk för Locums IT-system eller informationstillgångar.

12 Avsteg och dispens

Avsteg från denna riktlinje kan i undantagsfall beviljas av Vd efter skriftlig framställan till Locums säkerhetschef. Avsteg beviljas endast för en avgränsad tidsperiod.