|  |  |
| --- | --- |
|  | **Informationssäkerhetsregel för anställda** |
|  | **Version: 1** |
|  | **Beslutsinstans: Regiondirektör** |
|  |  |



**ÄNDRINGSFÖRTECKNING**

Var noga med att varje gång du ändrar i dokumentet skriva in vad du ändrat och byt versionsnummer. Se till att du också byter versionsnumret i sidfoten. Versioner räknas upp med 1 varje gång (1, 2, 3, 4). Använd TAB-tangent för att få ny rad.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Ändring** | **Beslutat av** |
|  |  | Nyutgåva |  |

**innehållsförteckning**

1 Inledning 4

1.1 Varför är regler för säkerhet viktigt? 4

2 Lösenord och inloggning 4

2.1 SITHS e-tjänstekort 5

2.2 Inloggningsuppgifter 5

2.3 Lösenordshantering 5

3 Distansarbete 6

4 Säker informationshantering 7

4.1 Tystnadsplikt 7

4.2 Sekretess 7

4.3 Hantering av IT-arbetsplats 8

4.4 Mobil IT-utrustning, telefoner 8

4.5 Loggning - du lämnar spår efter dig 9

4.6 Internetanvändning 9

4.7 Sociala medier 10

4.8 Tillgång till patientuppgifter 10

4.9 Molntjänster 10

4.10 Virus och skadlig kod 10

4.11 Lagring och bärbara media 11

4.12 Uppdatering av bärbara datorer 11

4.13 Programvara 11

4.14 Regler för e-post i sammandrag 12

4.15 Utskrifter 12

4.16 Bärbar PC 12

4.17 Hantering av fax 13

5 Informationssäkerhetsavvikelser 13

6 Kontaktvägar 13

7 Referenser 14

# Inledning

Denna regel gäller för samtliga medarbetare inom Region Jämtland Härjedalen (regionen). Tillämpliga delar gäller även för externa parter som konsulter/leverantörer.

Regeln är en sammanfattning av de olika regelverk som styr regionens informationshantering ur säkerhetssynpunkt. Dokumentet lämpar sig som en översiktlig introduktion om säkerhet till alla användare av regionens informationssystem. För fördjupade beskrivningar av olika områden hänvisas till referenser.

## Varför är regler för säkerhet viktigt?

Information är en viktig tillgång för regionen och ska ses som en resurs som vilken annan tillgång som helst. För att skydda informationen krävs ett säkerhetsmedvetande hos alla medarbetare. Denna regel syftar till att underlätta ett säkert arbetssätt vid hantering av information, både i IT-system och i övrigt.

Hur informationen hanteras av användarna är avgörande för vilken säkerhet som kan uppnås. Alla anställda, studenter, externa uppdragstagare och övriga medarbetare har en del av ansvaret för säkerheten i regionens informationshantering.

Övergripande syften med att upprätthålla rätt säkerhetsnivå är:

* Att inte sekretessbelagd information kommer obehöriga till del.
* Att information i IT-systemen finns tillgänglig och är läsbar när den behövs.
* Att det i efterhand går att spåra i IT-systemen vem som utfört vad och när.

Om dessa mål är uppfyllda kan regionen uppfylla sitt uppdrag och uppnå en säker och ändamålsenlig informationshantering som uppfyller verksamhetens krav och gällande lagkrav. Med ett tydligt regelverk blir det lättare att uppfylla kraven. Som användare behöver du informera dig för att uppfylla din del i arbetet och kunna känna dig trygg i din roll i informationshanteringen.

# Lösenord och inloggning

Regionens informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information.

Ansökan och beslut om behörighet ska göras enligt bestämda regler som kan variera något från system till system. Vänd dig till din chef om du behöver ny eller ändrad behörighet till något system. Chefen kan också ha delegerat till utsedda behörighetsbeställare att sköta beställningen av behörigheter.

## SITHS e-tjänstekort

Alla arbetstagare och studenter inom Region Jämtland Härjedalen och flertalet av de externa uppdragstagare som ska använda regionens IT-system tilldelas ett SITHS e-tjänstekort.

Ditt SITHS-kort är en identitetshandling som visar vem du är och att du arbetar inom Region Jämtland Härjedalen. Tänk på att det är en värdehandling och var aktsam så att det inte tappas bort. Du är personligt ansvarig för att kortet inte förloras och att du har det tillgängligt för att kunna utföra ditt arbete. Kortet används till inloggning i IT-system, inpassering och vissa typer av betalning.

När du slutar din anställning/uppdrag/studier inom Region Jämtland Härjedalen ska kortet återlämnas till närmaste chef eller till närmaste lokala SITHS-administratör för makulering.

Så här hanterar du ditt SITHS-kort:

* Lämna aldrig ditt kort eller dina koder åtkomligt för någon annan
* Ta alltid med dig kortet från IT-arbetsplatsen då du lämnar den
* Förvara alltid ditt kort och dess koder åtskilda från varandra
* Se till att alltid ha tillgång till din PUK-kod
* Om du förlorar ditt kort ska du omedelbart spärra det genom att kontakta regionens Helpdesk

Om du anger fel PIN-kod tre gånger i rad kommer kortet att låsas. Du kommer då att behöva använda din PUK-kod för att låsa upp kortet.

Utan dessa koder går ditt kort inte att använda. Ingen annan får känna till koderna och du måste själv hålla reda på ditt PIN-kodsbrev.

Mer information om kortet finns under SITHS på Insidan.

## Inloggningsuppgifter

När behörigheten är formellt beslutad och registrerad får du:

* En användaridentitet
* Ett lösenord - din egen hemlighet

Istället för lösenord kan ditt tilldelade SITHS-kort i flera fall vara din ”nyckel” (istället för lösenord) för att få åtkomst till ett system/en resurs där du blivit tilldelad behörighet. Detta gäller till exempel för inloggning till regionens Citrix-miljö.

Om du bara loggar in med kort och inte har behov av att kunna logga in med lösenord kan du be Helpdesk att ta bort lösenordet för Citrix.

När du fått din behörighet ansvarar du för att följa de regler (se nedan) som kopplas till behörigheten och ditt eventuella lösenord.

## Lösenordshantering

**Inloggning med SITHS-kort:** Inloggningen till Citrix-miljön sker normalt med SITHS-kort som vanligaste inloggningssätt. Vissa användare har dock fortfarande kvar möjligheten att kunna logga in med lösenord i Citrix från vissa klienter där detta inloggningssätt tillåts.

**Inloggning med lösenord:** Använder du lösenord till Citrix kommer du automatiskt att behöva byta detta minst var 90:e dag. Även i system som inte automatiskt kräver lösenordsbyte bör du byta minst var 90:e dag (varje kvartal) för att försvåra att ditt konto används för obehörig inloggning.

**Lösenordet är personligt:** Lösenordet är ditt privata, helt egna lösenord. Det är strängt personligt och i systemet kan man säga att du **är** ditt lösenord. Lösenordet ska hanteras med varsamhet och får inte lämnas ut till någon.

Du ska därför:

* Inte använda samma lösenord i arbetet som du har i privata applikationer, exempelvis Facebook.
* inte avslöja ditt lösenord för andra eller låna ut din behörighet
* skydda lösenordet väl
* byta lösenord minst var 90:e dag
* omedelbart byta lösenordet om du misstänker att någon känner till det
* välja ett lösenord med minst 8 tecken. Lösenordet måste uppfylla minst tre av följande kriterier:

Lösenordet ska innehålla minst ett tecken från minst tre av följande fyra grupper:

* versaler (A - Z)
* gemener (a - z)
* alfanumeriska tecken (0-9)
* specialtecken (såsom: !, $, # eller %)

**Om du glömmer ditt lösenord:** Försöker du att logga in flera gånger till systemet med ett felaktigt lösenord kommer ditt konto att spärras/låsas. Om ditt konto spärrats kan du själv låsa upp det via lösenordsfunktion som finns i Citrix-miljön (om du har tillgång till ditt SITHS-kort) eller få det öppnat igen av behörig systemadministratör vilket oftast (men inte alltid) är Helpdesk.

# Distansarbete

Arbete på distans ger större frihet i jobbet men ställer också nya krav på hur vi ska agera. Vid distansarbete ska du använda de tekniska lösningar som Region Jämtland Härjedalen erbjuder. Tänk på vad som visa på skärmen när du vistas i exempelvis tåg, restauranger mm. Lås datorn även om du lämnar den för en kort stund. Samma sak gäller i hemmet. Låt inte barn eller familj av misstag få möjlighet att ta del av känsliga uppgifter.

Den systemspecifika säkerhetsinstruktionen för användare ska ange vilka säkerhetsregler som gäller vid arbete på distans (via t ex PC i hemmet eller från mobil arbetsplats).

Särskilda krav ställs vid arbete med mobil utrustning. Bl. a ska undvikas att spara känsliga uppgifter på en lokal hårddisk. I särskilda fall kan bestämmelser om kryptering av uppgifter finnas angivna i systemets säkerhetsinstruktion. I de fall att filer lagras lokalt utanför regiongemensamma servrar ansvarar användaren själv för att säkerhetskopiering utförs åtminstone en gång per dygn om lagrade uppgifter har förändrats.

# Säker informationshantering

Detta avsnitt anger hur vi uppnår en säkrare hantering av verksamhetens information i våra IT-system. Krav som ska uppfyllas av verksamheten kommer dels direkt från brukare/medborgare och dels via gällande lagstiftning (bl. a Offentlighet- och sekretesslagen, Socialtjänstlagen, Arkivlagen och Personuppgiftslagen). De uppgifter som berörs här avser i första hand de som hanteras i verksamhetskritiska system och de som sekretessklassats. Även personuppgifter som berör den personliga integriteten berörs.

## Tystnadsplikt

Muntlig sekretess – dvs. tystnadsplikt gäller inom regionen enligt Offentlighets- och sekretesslagen för all offentlig vård och för privat hälso- och sjukvård regleras detta i 6 kap. 12-16§§ patientsäkerhetslagen (2010:659).

Känslig information eller personrelaterad information ska aldrig diskuteras på allmän plats eller då risk finns att obehöriga kan höra telefonsamtalet.

Brott mot tystnadsplikt – Den som uppsåtligt eller om utlämnande sker av oaktsamhet lämnar ut sekretessbelagda uppgifter som inte får lämnas ut kan dömas till böter eller fängelse i högst ett år. Vid obehörigt röjande kan disciplinpåföljd åläggas hälso- och sjukvårdspersonal.

## Sekretess

Sekretesskyddade uppgifter förekommer ofta inom regionen, inte minst gäller detta patientinformation inom hälso- och sjukvården.

Sekretess ställer krav på skyddsåtgärder så att uppgifter inte avsiktligt eller oavsiktligt görs tillgängliga eller avslöjas för obehöriga eller utnyttjas på ett otillåtet sätt.

För att upprätthålla sekretess vid lagring och överföring av information via IT-system krävs insynsskydd. Insynsskydd kan IT-tekniskt erbjudas på flera olika sätt, t ex genom reglerad åtkomst/behörighet till data (via personlig inloggning) och genom kryptering av meddelanden. Det dock alltid IT-användarna som genom sitt agerande i slutändan avgör om sekretessen ska kunna upprätthållas eller inte vid hantering av uppgifter i ett IT-system.

Tänk därför på att:

* Aldrig skicka sekretessklassade uppgifter via öppen e-post (vare sig internt JLL eller externt till brukare/medborgare)
* se alltid till att använda din egen inloggning/konto vid åtkomst till sekretess klassad information via IT-system
* avsluta/logga ut/lås ditt användarkonto då du inte använder kontot eller finns i närheten av din klient/IT-arbetsplats för att inte ge obehöriga åtkomst till sekretessuppgifter som kan nås via din registrerade behörighet

Olovlig åtkomst till sekretessuppgifter (i t ex patientjournaler) kan upptäckas i IT- system. Då det gäller regionens journalsystem registreras/loggas alla användare som haft åtkomst till sekretessuppgifter knutna till patienter. Den som olovligen bereder sig tillgång till IT-lagrade personuppgifter som täcks av Offentlighet- och Sekretesslagen kan dömas till böter eller fängelse för dataintrång.

## Hantering av IT-arbetsplats

Då du lämnar din klientarbetsplats ska du inaktivera din session genom att dra ut ditt SITHS-kort ur kortläsaren eller – om du loggar in med lösenord - låsa eller logga ut klienten. Ditt SITHS-kort ska alltid tas med då du lämnar klienten.

* **Tunn klient** - En aktiv session i Citrix kan låsas genom att dra kortet ur kortläsaren.
* **PC-klient** – På de klienter där inloggning med SITHS-kort kan ske kan klienten låsas och Citrix-sessionen inaktiveras genom att dra kortet ur kortläsaren. På övriga PC-klienter utan stöd för kortinloggning ska man välja Ctrl + Alt + Del och låsa PC:n då man lämnar klienten under en kortare tid. Lämnar man klienten längre tid ska man alltid logga ut helt.

Kom ihåg att du har ett ansvar för allt som registrerats med din inloggning/ användaridentitet!

## Mobil IT-utrustning, telefoner

Den som vill behandla personuppgifter i mobila enheter (till exempel surfplattor och smarta mobiltelefoner) måste vara medveten om att det kan innebära vissa särskilda risker. Risker som kan få svåra konsekvenser för en enskild vars personuppgifter riskerar att spridas. En mobil enhet kan kommunicera över öppna nätverk och används ofta utanför arbetsgivarens lokaler. Det finns möjlighet att ladda ned appar och utnyttja ett stort antal olika tjänster på en mobil enhet. Appar kan dock påverka säkerheten i den mobila enheten och medföra oavsiktlig spridning av personuppgifter.

Mobila enheter är som regel stöldbegärlig egendom. Om personuppgifterna i enheten inte är tillräckligt skyddade kan det vara svårt att avgöra om det är den behörige användaren som tar del av uppgifterna. Den personuppgiftsansvarige måste, så långt det är möjligt, vidta säkerhetsåtgärder för att bara en behörig användare ska få åtkomst till personuppgifterna i fråga.

Integritetskänsliga personuppgifter som lagras i en mobil enhet ska vara krypterade. Du måste kontrollera att informationen som lagras i den mobila enheten inte oavsiktligt kopieras och lagras i så kallade molntjänster. När det inte längre är nödvändigt att lagra uppgifterna i de mobila enheterna ska de raderas.

Du bör inte använda privata mobila enheter som tjänsteverktyg. Den personuppgiftsansvariges skyldigheter är samma även för anställda som tillåts använda sina egna mobila enheter.

Kontakta omedelbart Helpdesk vid förlust eller stöld så att IT kan fjärradministrera läsplattan, vid behov fjärradera den lagrade informationen och ta bort åtkomsten till regionens datanät.

## Loggning - du lämnar spår efter dig

Loggning innebär en registrering av händelser/transaktioner i IT-systemen. Loggarna används för uppföljning av bl. a. ta reda på vad som lagrats/skrivits, vem som gjorde det och när det utfördes.

När du är inloggad och arbetar i regionens IT-system lämnar du spår efter dig. Systemens loggningsfunktion används för att spåra obehöriga intrång. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänks i händelse av att oegentligheter skulle inträffa. Genom att gå igenom loggar kan systemansvariga följa upp att IT-systemen används på rätt sätt.

För mer information läs referens 5 Rutin för loggkontroll i vårdadministrativa system, Dnr: LS/450/2014

## Internetanvändning

Införandet av internettjänster i verksamheten är ett område där säkerheten påverkas i mycket hög grad av användarnas beteende. Regionens lokala nätverk är anslutet till Internet via en brandvägg som reglerar in- och utgående trafik. Loggning sker av trafiken genom brandväggen.

**Vid användande av Internet gäller följande:**

* Filer som innehåller spelprogram, musik och filmer får inte laddas ned och installeras i våra system. Förutom att dessa filtyper inte är förenliga med arbetsuppgifterna kan de innehålla skadlig kod.
* Andra program, oavsett om de är gratis eller inte, får **Inte** heller laddas in och installeras i regionens system utan att de virustestats och godkänts av ansvariga för IT-infrastrukturen.

Allmänt gäller att vid nedladdning av filer från Internet krävs att du har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välrenommerade webbplatser. Filer som laddas ner via Internet kontrolleras (scannas) automatiskt för att upptäcka och ta bort ev. virus. De filer som innehåller kända virus stoppas.

När du surfar på Internet representerar du organisationen. Du lämnar spår efter dig på Internet i form av organisationens nätverksadresser. Dessa adresser kan – i fel händer – användas av obehöriga för missbruk av nätverksresurser i regionens datanät.

Mer information om hur Internet används ges i Referens 2, ”Regler för webbanvändning”.

## Sociala medier

Region Jämtland Härjedalen har i grunden en positiv och öppen hållning till sociala medier.

* Användning av sociala medier ska vara förenligt med arbetsuppgifterna
* Användandet får inte skada Region Jämtland Härjedalens förtroende

Det är viktigt att göra klart i vilken egenskap man skriver, om man uppträder som privatperson eller i sin yrkesroll.

Läs mer: Referens 3: Regler för sociala medier Dnr: LS/1674/2012

## Tillgång till patientuppgifter

För att du som vårdpersonal ska ha rätt att ta del av patientuppgifter, exempelvis via ett journalsystem, krävs en vårdrelation. Då vårdrelationen är avslutad har du inte längre rätt att gå in i patientens journal. När det gäller att läsa journaluppgifter från andra vårdgivare, exempelvis från en privat vårdcentral, krävs också att patienten lämnar sitt samtycke.

Otillbörlig åtkomst till journaluppgifter räknas som dataintrång och är straffbar.

För mer information om när man har rätt att ta del av patientuppgifter, se referens 6 ”Rätt att ta del av patientuppgifter inom Region Jämtland Härjedalen, se även referens 7 ”Hantering av patientuppgifter för kvalitetssäkring inom vård och behandling”

## Molntjänster

Molntjänster innebär att exempelvis processorkraft, lagring och funktioner tillhandahålls av leverantörer som tjänster över Internet.

Den som använder en molntjänst för lagring av personuppgifter, till exempel i ett löneregister, förlorar den faktiska kontrollen över de personuppgifter som lagras. Till detta kommer att molnleverantörer ofta använder sig av standardavtal, det vill säga i förväg definierade användarvillkor, och anlitar underleverantörer. Det är därför viktigt att den som tänker använda en molntjänst i sin verksamhet är medveten om de krav som ställs enligt personuppgiftslagen.

Innan installering/användning av en molntjänst ska kontakt tas med regionens It-säkerhetsansvarig samt regionens informationssäkerhetssamordnare.

## Virus och skadlig kod

Virus och annan skadlig kod är idag ett stort problem. De vanligaste sätten en dator blir smittad på är via:

* USB-minnen
* Bifogade filer eller länkar i e-post
* Program hämtade från internet

Tecken på virusangrepp på klienten kan vara att:

* Datorn utför operationer/arbete utan att du själv initierat det, t ex förändringar sker på skärmen (tecken flyttas, försvinner etc.).
* Datorn uppträder på ett onormalt sätt, t ex arbetar mycket långsamt eller program går inte att köra.

Du kan som användare minimera risken genom att vara mycket återhållsam med vilka filer eller länkar du öppnar i e-posten. Vid minsta misstanke om att din dator är smittad ska du omedelbart kontakta Helpdesk.

## Lagring och bärbara media

Lagring av viktig eller känslig information ska alltid ske på en lagringsplats som är säker och där säkerhetskopiering (backup) sker. Lagring av patientuppgifter ska ske i regionens vårdsystem.

För lagring av filer finns användarens hemkatalog tillgänglig (H:/)samt gemensamma diskar (G:/).

På en dators lokala hårddisk (C:/) ska normalt ingen lagring ske. Förutom stöldrisken finns ingen säkerhetskopiering vilket innebär att informationen är borta om datorn går sönder eller blir stulen.

På flyttbara lagringsmedia som USB-minnen och portabla hårddiskar får ingen lagring ske av känsliga uppgifter. Dessa lagringsmedia ska betraktas som mycket osäkra eftersom det exempelvis är lätt att tappa bort ett USB-minne.

## Uppdatering av bärbara datorer

Då och då ger leverantören av operativsystem ut säkerhetsuppdateringar för att korrigera för upptäckta säkerhetsluckor. Dessa uppdateringar installeras automatiskt för alla fast ansluta klienter i regionens nät. För bärbara PC som används utanför regionnätet är det viktigt att med jämna mellanrum ansluta dessa till Internet för att de ska få installerat dessa uppdateringar och förbli ”säkra”.

## Programvara

Endast program som godkänts av Region Jämtland Härjedalen ska användas. Du har som användare inte rätt att installera egna program, eller sådana som hämtats från Internet. Vid behov av nya program ska du ta kontakt med regionens Helpdesk.

Det finns en stor risk för driftstörningar eller datavirus om du installerar okända programvaror, skärmsläckare, bakgrundsbilder etc.

Nedladdning av filer: Då en webbsida besöks och man klickar på en typ av länkar dyker ibland dialogrutor/”pop-up-fönster” upp, vilka uppmanar till att ladda ned en fil. Om du inte själv säkert vet vad filen innehåller ska du klicka på ”nej” eller ”avbryt”, och inte ladda ner filen. Som användare kan du i detta fall inte känna till innehållet i filen (det kan t ex vara ett virus).

## Regler för e-post i sammandrag

Nedan sammanfattas kort de säkerhetsmässigt viktigaste punkterna från dokumentet ”Regel för posthantering”, se Referens 1:

* Om du misstänker att det kommit in virus via e-postsystemet ska du agera som beskrivits i avsnittet om Internetanvändning (se avsnitt 4).
* Ämnesraden i ett e-postmeddelande ska inte innehålla känslig information. Innehållet i ämnesraden (”Ärende:” i FirstClass) loggas och kan potentiellt få större spridning till utomstående/obehöriga än själva meddelandetexten.
* E-post får för närvarande inte användas för att skicka sekretesskyddad information såsom patientuppgifter.
* Oönskad, massutskickad e-post, s.k. spam-meddelanden tar upp mycket lagringsutrymme, kan innehålla virus och bidrar till att skapa oreda i kommunikationen. Du kan själv bidra till att minimera antalet spam-meddelanden genom att tänka på att inte sprida din e-postadress mer än nödvändigt.

Mer information om e-post finns i Referens 1, ” Rutin för hantering av post i Jämtlands läns landsting – traditionell post, e-post, sms, fax och röstbrevlådor”.

## Utskrifter

Sker utskriftav dokument på en gemensam skrivare ska du hämta dokumentet så snart du kan. Gäller det utskrift av sekretessbelagda eller känslig uppgifter ska du ha skrivaren under uppsikt i väntan på utskrift och därefter omedelbart hämta dokumentet efter att utskriften är klar. Tänk på att kvarglömda dokument kan komma i orätta händer.

Glöm heller inte att kontrollera att rätt nätverksskrivare är vald för utskriften. Varje användare ansvarar för att han/hon har rätt skrivare inställd som sin standardskrivare.

## Bärbar PC

Bärbara persondatorersom du använder utanför din ordinarie arbetsplats utgör en säkerhetsrisk. Därför ska du:

* Hålla utrustningen och datamedia under ständig uppsikt om du inte kan låsa in den.
* Aldrig spara lösenord lokalt i den bärbara datorn.

Du får inte spara känslig och/eller verksamhetskritisk information på den bärbara datorn. All sådan information ska enbart lagras på gemensamma resurser i IT-infrastrukturen där den är väl skyddad och regelbundet blir säkerhetskopierad. Om du ändå måste spara annan *icke* verksamhetskritisk information på den bärbara datorn ansvarar du själv för att den blir säkerhetskopierad.

## Hantering av fax

Faxöverföring är mycket sårbar för obehörig åtkomst till information. Känsliga uppgifter, som exempelvis patientuppgifter, får enligt lag inte skickas okrypterat över ett öppet nätverk. Det innebär att du inte får skicka identifierbara patientuppgifter via e-post eller fax. Det är endast tillåtet i avidentifierad form.

Samma princip ska gälla även för annan information som inte specifikt räknas som patientuppgifter, men som ändå klassas som känsliga. Exempelvis kreditkortsuppgifter.

Mer information om faxanvändning finns i Referens 1,” Rutin för hantering av post i Jämtlands läns landsting – traditionell post, e-post, sms, fax och röstbrevlådor” samt referens 4 ”Rutin för faxhantering”.

# Informationssäkerhetsavvikelser

Informationssäkerhetsavvikelser är oavsiktliga eller avsiktliga händelser och risker som påverkar eller kan komma att påverka säkerheten negativt för Region Jämtland Härjedalens informationstillgångar. Exempel på sådana incidenter är brott mot sekretessen, allvarliga driftsavbrott, skadlig kod (virus) eller programvara, dataintrång eller obehörigt användande av information. Incidenter kan även vara förlust av dator eller lagringsmedia.

Säkerhetsskyddet är ytterst beroende av den enskilde medarbetarens lojalitet och ansvarstagande. Samtliga anställda har en skyldighet att rapportera risker, brister och incidenter avseende informationssäkerhet i regionens avvikelsesystem Centuri.

Vid rapportering ska det anges om ett IT- system är inblandat i händelsen. Det finns möjlighet att i fritext ange vilket IT- system som berörs.

Observera att avvikelserapporteringen inte ersätter behovet att anmäla ett fel i ett IT-system till Helpdesk. Akuta IT-incidenter som kräver omedelbara åtgärder ska direkt anmälas till IT-driftorganisationens support d.v.s. Helpdesk.

# Kontaktvägar

Behöver du hjälp med informationssäkerhetsfrågor eller vill du tipsa om något inom detta område? Kontakta regionens informationssäkerhetssamordnare, se uppgifter under Informationssäkerhet i ledningssystemet.

Generell rådgivning inom informationssäkerhet kopplat till användning av IT-system kan ges av regionens Helpdesk.

# Referenser

**Referens 1** Rutin för hantering av post i Jämtlands läns landsting – traditionell post, e-post, sms, fax och röstbrevlådor Dnr:RS/253/2015

**Referens 2** Regler för webbanvändning, dok. nr:16381

**Referens 3** Regel för sociala medier, Dnr: LS/1674/2012

**Referens 4** Rutin för faxhantering Dnr: LS/1010/2014

**Referens 5** Rutin för loggkontroll i vårdadministrativa system, Dnr: LS/450/2014

**Referens 6** Rätt att ta del av patientuppgifter inom Region Jämtland Härjedalen, Dnr, LS/1246/2014

**Referens 7** Hantering av patientuppgifter för kvalitetssäkring inom vård och behandling, Dok nr: 22960