Riktlinje för informationssäkerhet - Användare

Omfattning

Riktlinjen vänder sig till all personal i landstinget och anger riktlinjer för hur den anställde skall förhålla sig till säkerhet av information i anställningen.

Bakgrund

Styrande dokument för informationssäkerhetsarbetet är Västerbottens läns landstings informationssäkerhetspolicy och riktlinjerna Användare och Förvaltning och drift.

Syfte

Syftet med VLL:s riktlinjer för informationssäkerhet är att säkra hantering och bearbetning av information för att uppnå önskad tillgänglighet, riktighet, sekretess och spårbarhet samt säkerställa att informationen skyddas mot obehörig åtkomst. Målet med riktlinjen är att informationssäkerhetsorganisationen är tydligt definierad samt att riktlinjerna ger ett stöd i utformandet av rutiner på informationssäkerhetsområdet.

Lagar och andra krav

Tryckfrihetsförordningen (SFS 1949:105)
Offentlighets- och sekretesslagen (SFS 2009:400)
Personuppgiftslagen (SFS 1998:204)
Patientdatalag (2008:355) PDL
SOSFS 2008:14

Ansvar och befogenheter

Informationsanvändare

Samtliga anställda som i sin yrkesutövning hanterar information inom landstinget är informationsanvändare. Varje informationsanvändare ansvarar för att följa fastställda riktlinjer och rutiner samt att genast rapportera avvikelser, incidenter samt risker kopplade till informationssäkerhet.

Beskrivning

Vid anställning och avslut av anställning

I samband med anställning ska du som anställd få kunskap om informationssäkerhet och din roll i informationssäkerhetsarbetet och vad som händer om man bryter mot gällande informationssäkerhetsregler. Du ska få utbildning i informationssäkerhet och i de informationssystem som du ska använda i din tjänsteutövning. Utbildningen ska anpassas till de system och programvaror som är aktuella för tjänsten.

Innan du anställs kommer arbetsgivaren kontrollera din ev. legitimation och ev. disciplinärenden eller anmärkningar hos IVO. Du kommer att få ett SITHS-kort (ett aktivt elektroniskt ID-kort framtaget av SKL) för säker identifiering i VLLs vårdsystem.

Då du avslutar din anställning skall samtliga tillgångar (dator, telefon, nycklar etc.) återlämnas till arbetsgivaren.

Behörighet i informationssystem

Verksamhetschefen ansvarar för att du har rätt behörighet i verksamhetens informationssystem utifrån vad som behövs för att fullgöra dina arbetsuppgifter. Om du får nya arbetsuppgifter ska behörigheten ändras så att den stämmer överens med de nya arbetsuppgifterna.

Mobil datoranvändning och distansarbete

Känslig information ska endast hanteras i de specifika system som anvisats för denna hantering. För de fall information måste bearbetas på lokal dator eller lagringsmedia måste du som anställd följa de särskilda rutinerna för hur överföringen av information ska ske. Vid fjärranslutning till VLL:s interna datornät finns också särskilda rutiner. Enbart godkänd utrustning och mjukvara får användas inom landstingets IT-system.

Mobila enheter

Vid användning av mobila enheter skall du som användare alltid ha fysisk kontroll över enheten och aldrig lämna den obevakad. Du skall använda lösenordsskyddsfunktionen för den mobila enheten. Lösenordet skall vara kvalitativt. Den mobila enheten skall i första hand anslutas mot kända trådlösa nätverk. Du som användare får inte byta SIM-kort i enheten för privat ändamål eller hantera den på annat sätt som bryter mot VLLs regelverk. Du ska omedelbart meddela arbetsgivaren om en mobilenhet blivit stulen eller på annat sätt förlorats.

Användning av Internet

Man får som användare inte upprätta egna anslutningar till Internet, utan endast ansluta till Internet genom landstingets nätverk och dess godkända kopplingspunkter. Användning av internet ska ske för ändamål som har med arbetsuppgifterna att göra. Vid användande av internettjänster ska agerandet vara sådant att det inte uppstår en förtroendeskada för landstinget. Användaren får heller inte använda Internet på ett sådant sätt att landstingets nätverk utsätts för väsentlig belastning eller andra säkerhetsrisker eller står i strid med gällande lagstiftning.

Loggning av landstingets internettrafik sker. I syfte att upprätthålla säkerheten och minska risken för att landstinget utsätts för skadlig kod samt att minska risken för olagliga internetbesök, har landstinget infört ett webbfiltersystem som övervakar all internettrafik. I webbfiltersystemet sker blockning av webbsidor som bryter mot riktlinjerna om informationssäkerhet. Spårning och analyser av enskilda datorer och användare kan göras i systemet. Landstinget dekrypterar innehållet både in och ut.

Landstinget kan på detta vis ta del av alla anställdas internetanvändning. Se även rutinen för användning av Internet.

Loggkontroll

Loggning definieras som registrering av de handlingar och aktiviteter som utförs i ett IT-system inklusive vilken information som skapats, lästs eller överförts. Alla användare som använder ett system loggas och det görs uppföljningar av loggarna i form av loggkontroller. Det är därför viktigt att du bara tar del av den information som du behöver i ditt arbete i systemen.

Lösenordshantering

Lösenord är personliga och rutiner för lösenord ska finnas för respektive IT-system. Rutinen skall säkerställa att lösenordet är kvalitativt och att lösenordet byts ut regelbundet. Du som användare skall säkerställa att ditt lösenord skyddas mot obehöriga.

Försändning av sekretessbelagd information

Vid intern försändning av sekretessbelagd elektronisk information via e-post ska landstingets upprättade riktlinjer och rutiner för e-post följas. Vid postförsändelse ska sekretessbelagd information skickas som rekommenderat brev eller paket. Fax skall normalt sett inte användas vid försändning av sekretessbelagd information. Användning av fax kan ske endast i undantagsfall, när annan metod för överföring inte är möjlig. Verksamhetschefen för den basenhet som berörs ska fastställa styrande eller vägledande dokument och göra dessa kända i verksamheten om fax kan användas för en viss typ av handling och/eller situation vid den egna enheten. För de fall en verksamhet använder fax frekvent i kommunikation med andra myndigheter skall verksamhetschefen även överväga att införskaffa en sk. Kryptofax genom MSB för säker överföring av information.

I första hand skall sekretessbelagd information avidentifieras innan det sänds. Om sekretessbelagt eller integritetskänsligt material sänds via fax måste särskilda skyddsåtgärder vidtas för att säkerställa att ingen obehörig kan komma att nås av uppgifterna.

- Den som sänder sekretessmaterial via fax har ansvar för att kontrollera att materialet når fram till rätt person på ett säkert sätt. Samt att det faxnummer som används stäms av med mottagaren.
- Sändaren ska säkerställa att mottagaren har uppsikt över faxen
- Sändaren skall i så hög utsträckning det är möjligt använda sig av förprogrammerade nummer
- Före sändningen bör mottagarens nummer kontrolleras och efter sändningen bör det kontrolleras att sändningen har genomförts utan anmärkning.
- Telefaxen bör placeras i låst utrymme eller så att den ansvarige har uppsikt över den.
- Ett försättsblad, som anger till vem faxet är, varifrån det kommer och hur många sidor som sänds, ska alltid användas
- När hel eller delar av patient journal sänds ska i enlighet med patientdatalagens krav alltid anteckning göras i journalen att uppgifter lämnats och till vem

Korrespondens med patienter

Alla försändelser ska sändas till patientens aktuella folkbokföringsadress. Det ska finnas särskilda rutiner vid kontakt med patienter som har skyddade personuppgifter.

Personuppgiftsbehandlingar

Samtliga personuppgiftsbehandlingar inom landstinget skall föras in i en förteckning. En sådan

behandling av personuppgifter ska rapporteras till personuppgiftsombudet. För personuppgiftsbehandlingar som sker av extern part för personuppgiftsansvariges räkning skall personuppgiftsbiträdesavtal tecknas. Personuppgiftsombudet är ansvarig att bistå med hjälp för upprättande av sådana avtal.

Sekretess

Inom den offentliga sektorn är sekretess för anställda reglerad i offentlighets- och sekretesslagen. Du ska vid din anställning få information om sekretesslagstiftningen. Tystnadsplikten som följer av lagen gäller alla som arbetar med patienter, såväl vårdpersonal som administrativ personal, studenter, praktikanter, konsulter och förtroendevalda med flera. Det innebär dels att det finns en inre sekretess, du får bara ta del av den information som du behöver för att kunna utföra dina arbetsuppgifter och du får inte sprida den information du tar del av utanför arbetsplatsen. Detta gäller även efter att du avslutat din anställning.

Risk- och Avvikelsehantering

En säkerhetsbrist eller en avvikelse i informationssäkerheten ska rapporteras till närmaste chef. En avvikelse ska även hanteras enligt landstingets rutiner för avvikelsehantering.

Dokumentation och arkivering

Ej tillämpbart.

Historik

Dokumentet ersätter tidigare dokument nummer 99350, 83619, 83618, 83617, 83615, 83609, 83415

Utarbetat av

Personuppgiftsombud i samråd med informatikenheten och verksamhetsutvecklingsenheten.

Referenser och förändringar

Avsnittet placeras sist i dokumentet och hanteras av systemet

Dokumentinformation
Referenser: Nej
Förändringar sedan senaste utgåva: