Riktlinje för informationssäkerhet, förvaltning och drift

Omfattning

Riktlinjen vänder sig till landstingets ledning samt till förvaltningsorganisationen av informationssäkerhetsarbetet. Riktlinjen omfattar riktlinjer för organisation och förvaltning av informationssäkerhetsarbetet regler för systemutveckling, systemunderhåll och incidenthantering samt drift och underhåll av IT-system.

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.

Lagar och andra krav

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

Mål och uppföljning

Målet med riktlinjen är att informationssäkerhetsorganisationen är tydligt definierad samt att riktlinjerna ger ett stöd i utformandet att rutiner på informationssäkerhetsområdet. Informationssäkerhetsarbetet ska följas upp årligen genom att en rapport om informationssäkerhet tillförs patientsäkerhetsberättelsen. Rapporten ska innehålla de uppgifter som framgår av SOSFS 2008:14, dvs. vilka granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med informationssäkerhetspolicyn, vilka riskanalyser som har utförts avseende informationssäkerheten samt vilka förbättringsåtgärder som har vidtagits.

Ansvar och befogenheter

Landstingsfullmäktige

Landstingsfullmäktige har det övergripande ansvaret för informationssäkerhetsarbetet i landstinget och skall fastställa policy för informationssäkerhetsarbetet.

Styrelse och nämnder

Landstingsstyrelsen har utifrån reglementet i uppgift att styra och samordna förvaltningen av

landstingets angelägenheter och har uppsikt för hela landstingets utveckling och ekonomiska ställning. Styrelsen skall ta initiativ till utveckling av arbetsformer, system och rutiner. Styrelsen har även det övergripande ansvaret att se till att verksamheten arbetar i enlighet med de av fullmäktige beslutade dokument. Styrelsen har vidare ansvar för de informationssystem som stödjer landstingets verksamhet. Utifrån detta ansvar ska Styrelsen säkerställa att riktlinjer för informationssäkerhet finns i verksamheten samt att dessa följs. Styrelsen ska därmed även årligen säkerställa att en årsrapport om informationssäkerhet upprättas samt att det utifrån rapporten vidtas nödvändiga åtgärder. Årsrapporten skall biläggas patientsäkerhetsberättelsen.

Styrelsen och nämnderna är även personuppgiftsansvarig enligt definitionen i 3 § personuppgiftslagen. I detta ingår ansvar för att landstingets arbete med informationssäkerhet sker på ett ändamålsenligt sätt och i enlighet med fastställda riktlinjer, att nödvändiga resurser avsätts för samordningen av informationssäkerhetsarbetet samt att fastställa regler och riktlinjer för informationssäkerhetsarbetet.

Verksamhetschef

Ansvar för informationssäkerhet följer med verksamhetsansvar. Verksamhetschef eller motsvarande är därmed ansvarig för informationssäkerheten inom sin verksamhet. Verksamhetschefen ansvarar för att det finns rutiner för regelbunden granskning av verksamhetens informationssäkerhet. Rutinerna ska säkerställa att verksamheten uppfyller landstingets krav på informationssäkerhet.

All information som skapas inom landstinget skall ha en ägare. Verksamhetschefen är också informationsägare för den information som skapas och används inom verksamheten. Ansvaret innefattar att informationen har rätt kvalitet för sitt ändamål, finns tillgänglig då den behövs och att sekretesskänslig information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas på ett riktigt sätt. För information som hanteras i gemensamma IT system utövar informationsägaren ansvaret genom att tillse att information som tillförs systemet uppfyller informationssäkerhetskraven samt att kravställa gentemot berörda systemägare så att systemen uppfyller informationssäkerhetskraven. Verksamhetschefen har även planeringsansvar för lokala kontinuitetsplaner för informationssäkerhet. Verksamhetschefen ska tillse att medarbetarna får nödvändig information och utbildning gällande regler för informationssäkerhet.

Verksamhetschefen skall årligen genom patientsäkerhetsberättelsen rapportera de risker, analyser och genomförda åtgärder som vidtagits i verksamheten utifrån dess informationssäkerhetsansvar.

Systemförvaltning

Förvaltningen av IT system sker genom landstingets systemförvaltningsmodell.
Varje IT system i landstinget skall ha en systemägare. Systemägaren har ansvaret för respektive IT-systems säkerhet och ansvarar även för framtagande av kontinuitetsplaner för systemet. Systemägare

är beställare av informationssystem med det yttersta ansvaret att tillse att ett förvaltningsobjekt fungerar på avsett sätt. Systemägaren har befogenhet att fatta avgörande beslut om förvaltningsobjektet vid nyutveckling, vidareutveckling, förvaltning och avveckling utifrån landstingsövergripande beslut. Systemägaren ska utifrån sitt ansvar för informationssäkerheten upprätta rapport ”Årsrapport systemförvaltning”, årsrapporten ska tillföras informationssäkerhetsrapporten som är en del i den patientsäkerhetsberättelse som nämnder och styrelsen årligen skall ta del av.

Personuppgiftsombud

Varje nämnd utser personuppgiftsombud. Personuppgiftsombudet ska självständigt se till att landstinget behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister till nämnderna. Om rättelse inte vidtas efter påpekande, ska personuppgiftsombudet anmäla förhållandet till Datainspektionen. Personuppgiftsombudet ska även samråda med Datainspektionen vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas.

Beskrivning

Personaladministration

Anställning och avslut av anställning

Vid rekrytering får endast sådana personuppgifter som är nödvändiga för rekryteringen behandlas. I samband med nyanställning ska all personal få kunskap om informationssäkerhet och deras roll i informationssäkerhetsarbetet. Beställare/uppdragsgivare ska upprätta sekretessförbindelse för konsulter/entreprenörer med uppdrag inom VLL, innan uppdraget startar. All personal skall också veta vad som händer om man brutit mot gällande informationssäkerhetsregler. Det ska i varje verksamhet finnas rutiner/checklistor för avslutande av anställning.

All personal ska ha regelbunden utbildning i informationssäkerhet och i de informationssystem som de ska använda i sin tjänsteutövning. Utbildningen ska anpassas till de system och programvaror som är aktuella för tjänsten. Externa uppdragstagare ska följa VLL:s riktlinjer och uppfylla de krav på informationssäkerhet som gäller inom VLL.

Kontroll av legitimerad personal

Kontroll av legitimationer, specialistkompetens/-behörighet, eventuella disciplinärenden eller anmärkningar samt om en individ är under utredning av Inspektionen för vård och omsorg, skall alltid göras innan anställning.

Säker identifiering av personal

All hälso- och sjukvårdspersonal ska vara säkert identifierad (användar-ID). Alla användare av

landstingets IT-system ska ha en unik identitet som i regel baseras på HSA-ID, en identitet konstruerad utifrån Hälso- och Sjukvårdens Adressregister. Identiteten ska på ett säkert sätt verifieras elektroniskt, i landstingets vårdinformationssystem skall personalen använda SITHS, ett aktivt elektroniskt ID-kort framtaget av SKL.

Behörighetsadministration

Respektive verksamhetschef ansvarar för att dess personal har rätt behörighet. Verksamhetschefen har ett ansvar att begränsa behörigheter i journalsystem och i andra system med känsliga personuppgifter, till vad som behövs för att fullgöra sina arbetsuppgifter, att behörigheten är tillräcklig men samtidigt inte mer omfattande än vad som är nödvändigt. Detta gäller även externa personer som tilldelas behörigheter till IT-system. Om en användare får nya arbetsuppgifter ska behörigheten följas upp och förändras så att den stämmer överens med de nya arbetsuppgifterna.

Behörighet skall tilldelas efter en analys av vilken information olika personalkategorier i olika verksamheter behöver. Riskanalysen ska ta hänsyn till vilka risker det kan innebära om personalen har för lite eller för mycket tillgång till olika patientuppgifter. Vissa patientuppgifter kan kräva särskilda riskbedömningar, till exempel personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer samt uppgifter från vissa mottagningar eller vissa medicinska specialiteter. En riskanalys skall också göras för att belysa olika slags risker förknippade med för omfattande tillgänglighet. Då behoven varierar mellan olika typer av verksamheter ansvarar verksamhetschefen för att en behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14 genomförs på enhetsnivå. Dokumentation av genomförd behovs- och riskanalys arkiveras på enheten.

Det ska finnas dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter i samtliga IT-system. Förutom regelbunden kontroll av användarnas behörighetsbehov ska översyn av behörigheter ske efter organisations- eller systemförändring. Vid systemförändringar skall systemägaren informera berörda verksamhetschefer om detta. Behörighetsnivåer i samtliga system ska vara kopplade till personliga användaridentiteter.

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 ska vara informerade om att loggning sker och att det sker uppföljning i form av loggkontroller.

Användar-ID ska kunna användas för att spåra aktiviteter kopplade till den ansvariga individen. Loggar ska skyddas mot radering, manipulering och obehörig åtkomst. Rutiner för loggkontroll skall utformas för samtliga IT-system inom VLL, systemägaren ansvarar för att så sker. Av rutinen ska det framgå på vilket sätt, hur ofta loggarna ska granskas, vem som ska utföra granskningen, vad som är att betraktas som en överträdelse samt hur överträdelser ska hanteras. Loggningsverktyget och logginformationen

skall skyddas mot manipulation och obehörig åtkomst. Systemadministratörers och systemoperatörers aktiviteter ska loggas och skyddas och granskas regelbundet.

Fysisk säkerhet

Hantering av tillgångar

Tillgångar som är relaterade till information och informationsbehandlingar ska identifieras och en förteckning över dessa tillgångar ska upprättas och underhållas. Tillgångarna skall ha en ägare. Alla anställda och externa användare ska återlämna landstingets tillgångar som de förfogar över då anställning, uppdrag eller avtal har upphört.

Allmänt om skydd av utrustning och information

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Känslig elektronisk utrustning eller utrustning som behandlar känslig information ska placeras så att tillträde minimeras och utformning av lämpliga skyddsåtgärder underlättas. Kritiska IT-system och informationstillgångar ska inrymmas i säkra utrymmen, med adekvata skal- och brandskydd, ha säkerställd tillgång till el och kyla, samt adekvata tillträdesskydd och kontroller. Mobila enheter (telefoner och surfplattor) skall förvaras säkert, det skall finnas rutiner i verksamheten om vilka säkerhetskrav användaren skall vidta vid användning av en mobil enhet.

Tillträdesskydd

Tillträdesskydd ska säkerställa att obehöriga inte kommer i kontakt med känslig eller verksamhetskritisk information eller utrustning. Entréer till utrymmen där det finns känslig eller verksamhetskritisk information eller utrustning ska skyddas med bemannade receptioner eller datoriserade passagekontrollsystem. Till passagekontrollsystemen används individuella passerkort med kod, som ger möjlighet till loggkontroller av in- och utpasserande.

Brandskydd

För brandskydd av lokaler där det finns utrustning och information ska fastställda riktlinjer och rutiner för brandskydd inom VLL följas.

Vattenskydd

I säkra utrymmen bör det inte finnas vattenledningar. Finns det risk för vattenskador i ett säkert utrymme ska det finnas vätskealarm.

Kraftförsörjning och el-miljö

Elektronisk utrustning ska skyddas mot elavbrott och andra störningar i elförsörjningen. Strömförsörjning av verksamhetskritiska system och utrustningar ska ske via avbrottsfri kraft (UPS), som i sin tur bör anslutas till reservkraft. Regelbundna tester ska säkerställa att övergången till

reservkraft fungerar.

Underhåll av utrustning

Leverantörens rekommenderade underhållsplan för utrustningen ska följas. Undantag får endast ske om det finns fastställda rutiner för detta.

Säkerhet för utrustning utanför egna lokaler

Det ska finnas rutiner för hur utrustning och information får hanteras utanför de egna lokalerna. Vid utformning av rutiner och skyddsåtgärder ska det beaktas att riskerna kan variera mellan olika platser och olika tidpunkter.

Märkning

All utrustning förutom sådan som klassas som förbrukningsmateriel ska vara stöldskyddsmärkt innan den tas i bruk. Kontroll av märkningen ska göras i samband med respektive verksamhets årliga inventering. Verksamhetschefen ansvarar för denna inventering.

Omfördelning eller kassering av hårdvara

Vid kassering eller omfördelning av utrustning som behandlar sekretessbelagd information ska lagringsmediet tas ut och fysiskt förstöras enligt fastställd rutin från Informatikenheten. För övrig utrustning raderas lagringsmediet med hjälp av anvisade programverktyg innan den omfördelas eller kasseras.

System och drift av IT-system

Säkerhetskrav på systemmiljön

Landstinget ska ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer. Säkerhetsreglerna för produktionsmiljöerna ska i alla relevanta delar även gälla för utvecklings- och testmiljöerna.

Externa leverantörer

Varje leverantör som hanterar information genom tillgång, behandling, lagring, kommunikation eller tillhandahåller infrastrukturkomponenter ska genom avtal framgå alla relevanta informationssäkerhetskrav. Vid köp av IT-tjänster eller vid drift eller underhåll hos en extern part ska samma informationssäkerhetskrav gälla som om landstinget bedrivit verksamheten i egen regi. Krav ska ställas på att hantera informationssäkerhetsrisker som är relaterade till informationssäkerhetsarbetet. Om informationen i systemen innehåller personuppgifter ska parternas roller som personuppgiftsansvarig och personuppgiftsbiträde regleras genom ett personuppgiftsbiträdesavtal mellan parterna. Landstinget ska regelbundet granska och följa upp leverantörernas tjänsteleveranser.

Systemdokumentation

Det ska finnas systemdokumentation för varje IT-system. Dokumentationen ska normalt bestå av installations- och konfigurationsdokumentation, teknisk systemförvaltningsdokumentation samt användardokumentation. Dokumentationen ska vara fullständig och aktuell. Ändringar av dokumentationen ska ske enligt fastställda rutiner. Det ska även finnas rutiner för säkerhetskopiering av systemdokumentation. Arkivering av systemdokumentation ska ske i enlighet med Arkivlagen.

Godkänd utrustning och mjukvara

Enbart godkänd utrustning och mjukvara får användas inom landstingets IT-system. Det ska inom landstinget finnas rutiner för hur utrustning och mjukvara ska hanteras och användas.

Mobil datoranvändning och distansarbete samt mobila enheter

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 ska det finnas rutiner för hur hanteringen och överföringen av information ska ske. Vid fjärranslutning till VLL:s interna datornät ska det finnas upprättade rutiner.

Ändring i informationssystem

Förändring av informationssystem ska noggrant planeras och föregås av en riskanalys. Ändringar som riskerar att påverka informationssäkerheten ska testas i separat testmiljö innan de införs i produktionsmiljön. Alla IT-system ska ha rutiner för ändringshantering, vilka ska säkerställa att det är möjligt att återställa systemet till hur det såg ut före ändringen. Enbart de förändringar som utgår från systemförvaltningsplanen ska genomföras.

Säkerhetskopiering

Säkerhetskopieringen syftar till att all väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner. Undantaget är den information som tillförts systemet efter senaste säkerhetskopiering. Hur stor informationsförlust som kan accepteras definieras för varje system och tillämpning. Informatikenheten utformar rutiner för säkerhetskopiering av information för IT-systemen. Systemägaren skall regelbundet kontrollera säkerhetskopieringen.

Användning av privilegierade verktygsprogram

Användning av verktygsprogram som kan kringgå säkerhetsåtgärder i system och tillämpningar ska begränsas och styras strikt. Tillgången till källkod för program skall begränsas.

Akut incidenthantering

Allvarliga händelser i produktionsmiljön kräver ofta att åtgärder vidtas omgående där de fastställda rutinerna för ändringshantering kan behöva frångås. Sådana akuta åtgärder ska alltid dokumenteras och i efterhand följas upp enligt rutiner för ändringshantering.

Kontinuitetsplanering

Varje IT-system ska ha en kontinuitetsplan som säkerställer att kravet på tillgänglighet uppfylls även om systemet ligger nere.

Nätverk och internetanvändning

Säkerhetskrav på nätverksmiljön

Systemägaren har ansvar för att informationsöverföring inom systemet sker på ett säkert. Varje nätverk ska vara utformat så att det finns definierade gränssnitt, såväl fysiskt som logiskt, mot andra nätverk. Nätverk får endast sammankopplas efter genomförd riskanalys och nödvändiga skyddsåtgärder har vidtagits. En sådan riskanalys skall även göras utifrån ett tillgänglighet, riktighet, sekretess och spårbarhet perspektiv. Det ska finnas systemskisser över samtliga komponenter som ingår i nätverket och alla anslutningspunkter gentemot andra nätverk ska vara tydligt utmärkta.

Utveckling och tillämpning av e-tjänster

Innan beslut fattas om att använda en e-tjänst ska en riskbedömning göras utifrån den personuppgiftsbehandling som skall utföras. Bedömningen ska grunda sig i de grundläggande principerna om informationssäkerhet (tillgänglighet, riktighet, sekretess och spårbarhet) samt om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga, om personuppgifter kan komma att lämnas över till ett tredjeland och om den överföringen i så fall har stöd i personuppgiftslagen samt vilken annan lagstiftning som behöver beaktas vid behandlingen. En bedömning ska även göras av vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas. Sådana tjänster ska även föregås av säker identifiering av samtliga användare.

Trådlösa nätverk

I samband med att information överförs med hjälp av trådlösa nätverk ska kommunikationen krypteras. Verksamhetschefen för Informatik ska ansvara för att rutiner finns dels för hur det trådlösa nätverket ska vara konstruerat och vad som gäller vid användandet av det trådlösa nätverket.

Skydd mot datavirus

Verksamhetschefen för Informatik är ansvarig för att det finns utarbetade rutiner och uppställda krav på mjukvaruskydd mot skadlig kod, antivirusprogram.

Användning av Internet

Loggning av landstingets internettrafik ska ske och sparas. Informatikenheten ansvarar för att rutin för loggning finns.

Lösenordshantering

Lösenord är en av de vanligaste metoderna att validera en användares rätt till åtkomst av ett

informationssystem. Lösenord är personliga och användaren skall få information om hur man konstruerar ett säkert lösenord. Rutiner för lösenord ska upprättas av systemägare för respektive IT-system. Rutinen skall säkerställa att lösenordet är kvalitativt och att det byts ut regelbundet.

Webbfilter

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.

Avvikelsehantering

Informationssäkerhetsarbetet i landstinget ska bedrivas förebyggande för att eliminera risker för brister i informationens tillgänglighet, skydd, riktighet och spårbarhet. Ledningssystemet ska säkerställa att det finns rutiner för risk- och avvikelsehanteringen. Detta inkluderar även riskanalyser för att identifiera hot.

Respektive verksamhetschef ansvarar för att det finns rutiner för att säkerställa att informationssäkerhetsavvikelser och säkerhetsbrister hanteras på ett effektivt sätt så snart de har rapporterats. Varje informationsanvändare ansvarar för att följa fastställda riktlinjer och rutiner samt vara uppmärksam på att genast rapportera avvikelser till närmaste chef.

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

Uppge hur, var och av vilken befattning eller funktion som eventuell dokumentation och arkivering av resultat ska göras.

Historik

Dokumentet ersätter tidigare dokument nummer 99350, 83619, 83618, 83617, 83615, 83613, 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: