Policy för informationssäkerhet

Landstingsdirektörens stab
augusti 2015

LANDSTINGET BLEKINGE

Innehållsförteckning

Inledning och bakgrund

Information av olika slag är en alldeles nödvändig förutsättning för att landstinget ska nå sina verksamhetsmål. Den totala mängden information och utbytet av information ökar i omfattning både inom och mellan olika verksamheter i landstinget liksom mellan landstinget och andra organisationer, allmänheten, förtroendevalda och andra intressenter.

Landstingets verksamhet och trovärdighet får inte äventyras på grund av brister i informationshanteringen. Avbrott i informationsförsörjningen kan vara kritisk för verksamheten och felaktig information kan äventyra patientsäkerheten. Det är därför mycket viktigt att informationshanteringen skyddas från avsiktliga och oavsiktliga störningar. Information som rör enskilda personers sociala, medicinska och andra personliga förhållanden måste skyddas noga mot oönskad förändring, förlust och avslöjande. Detta gäller också information om andra patientspecifika uppgifter. Lagar och föreskrifter ska självklart följas.

Modern informationsteknik ger hög tillgänglighet till information och ger förutsättningar för landstinget att effektivisera och förbättra servicen till länets invånare. Beroendet av komplexa tekniska informationssystem innebär emellertid också ökad sårbarhet. Det är därför nödvändigt att ställa rätt krav på säkerhetslösningar vid upphandling, utveckling och användning av informationssystem och att fortlöpande kontrollera att dessa krav efterlevs.

Syfte

Arbetet med informationssäkerhet måste vara medvetet och strukturerat med tydliga mål och riktlinjer. Denna policy beskriver de övergripande principerna för informationssäkerhet. Policyn gäller för all informationshantering i Landstinget Blekinge oavsett om den hanteras manuellt eller med IT-stöd.

Mål

Informationssäkerheten är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder för att skydda informationen mot de hot den kan utsättas för.

Skyddsområden och mål:

- Tillgänglighet – att informationen finns till hands när den behövs
- Sekretess – att informationen bara är åtkomlig för den som har rätt att ta del av den
- Riktighet – att informationen är och förblir korrekt, begriplig och fullständig
- Spårbarhet – att man i efterhand kan identifiera vem som gjort vad och när

Informationssäkerhetsarbetet utgår från verksamhetens, lagars och föreskrifters krav utifrån ovanstående fyra perspektiv.

Genomförande

Skyddsåtgärder

Landstinget ska beskriva och införa organisatoriska, administrativa och tekniska skyddsåtgärder för vart och ett av ovanstående skyddsområden. Skyddsåtgärder ska dokumenteras på ett sådant sätt att det är möjligt att kontrollera att nödvändig skyddsnivå uppnås.

Val av skyddsåtgärder ska anpassas efter verksamheten och baseras på informationens betydelse och de konsekvenser som bristande säkerhet kan innebära för alla intressenter i en viss informationshantering. Lagar och förordningars krav ska utgöra lägsta nivå vid specificering av skyddsåtgärder.

En förutsättning för arbetet med informationssäkerhet är att en god säkerhetskultur genomsyrar hela verksamheten. Med detta menas att inte bara medarbetare har god kunskap om vilka säkerhetsregler som gäller, utan också att de kritiskt ifrågasätter händelser som kan påverka säkerheten.

Ansvar

Landstingsfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för landstinget.

Landstingsfullmäktige uppdrar till Landstingsstyrelsen, som i sin tur ger Landstingsdirektören i uppdrag att ansvara för omfattning och inriktning av landstingets informationssäkerhetsarbete. Detta sker genom fastställande av organisation och riktlinjer för informationssäkerhet. Landstingsdirektören ser även till att informationssäkerhetspolicyn och tillhörande riktlinjer revideras vid behov.

Ansvaret för informationssäkerheten ska vara kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten inom den verksamheten.

Den som ingår avtal som innefattar informationsutbyte ansvarar för att kraven på informationssäkerhet specificeras i avtalet.

Varje anställd ansvarar för att följa säkerhetsregler och att rapportera fel och störningar i informationssystem, utrustningar och informationsinnehåll enligt fastställda rutiner.

Informationssäkerhetsstrateg verkställer samordningen av informationssäkerhetsarbetet inom landstinget och förvaltar denna policy, de tillhörande riktlinjerna och tillämpningsanvisningarna samt den övergripande handlingsplanen för informationssäkerhet

Undantag

Landstinget Blekinge beslutar att göra ett undantag enligt SOSFS 2008:14 2 kap. § 5 genom att tillåta att påminnelser och kallelser till vård och behandling kan med patientens medgivande överföras via öppna nät t ex med sms.

Riktlinjer, föreskrifter och instruktioner

Denna policy ska konkretiseras i riktlinjer, och i förekommande fall, i interna föreskrifter (beslut), Instruktioner/rutiner. Dessa dokument bör så långt möjligt utformas och inbördes ordnas i enlighet med vedertagen internationell och svensk standard för informationssäkerhet (SS-ISO/IEC 27001, "Ledningssystem för informationssäkerhet").

Uppföljning

Denna policy ersätter nuvarande IT-säkerhetspolicy (dnr 111/10). Policyn bör revideras 2020.