Dokumentnamn: Policy för informationssäkerhet och dataskydd		Revision: 01
Dokumenttyp: 8.2.1.1.1 riktlinjer	Dokumentnummer: 19-75	
Detta dokument gäller för: Region Blekinge	Funktionsområde: Informationssäkerhet	
Dokumentansvarig: Informationssäkerhetsstrateg	Beslut av: Regionfullmäktige	
Beslut datum: 2019-04-10	Nästa revidering: 2020-03-31	

Policy för informationssäkerhet och dataskydd

Innehåll

Inledning

Information av olika slag är en viktig och nödvändig förutsättning för att Region Blekinge ska nå sina verksamhetsmål. Den totala mängden information och behovet av att utbyta information ökar i omfattning både inom och mellan olika verksamheter i regionen liksom mellan regionen och andra myndigheter, organisationer, allmänheten, förtroendevalda och andra intressenter. Dataskyddsförordningen har också krav på hur integriteten för de registrerades personuppgifter ska behållas.

Region Blekinges verksamhet och trovärdighet får inte äventyras på grund av brister i informationshanteringen. Avbrott i informationsförsörjningen kan vara kritisk för verksamheten, oavsett vilket område, exempelvis kan felaktig information 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 annan sekretesskyddad information som kan skada regionen. Lagar och föreskrifter ska självklart följas.

Modern informationsteknik ger hög tillgänglighet till information och ger förutsättningar för att effektivisera och förbättra servicen till länets invånare. Komplexa tekniska informationssystem med ökad tillgänglighet innebär en ökad sårbarhet. Det är därför nödvändigt att ställa rätt krav på säkerhetslösningar vid upphandling, utveckling och användning av informationssystem ur informationssäkerhets- och dataskyddsperspektiv. Uppföljning ska ske regelbundet.

Syfte

Syftet med policyn är att delge ledningens inriktning och stöd. Arbetet med informationssäkerhet och behandling av personuppgifter ska vara medvetet och strukturerat utifrån nedanstående mål och principer för informationssäkerhet och dataskydd. Policyn gäller för all informationshantering i Region Blekinge oavsett om den hanteras manuellt eller med IT-stöd och är en del av säkerhetsskyddet.

Mål

Informationssäkerhet

- Målet med informationssäkerhetsarbetet är att säkerställa ett lämpligt skydd för informationen i verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för Region Blekinges verksamheter att uppnå sina mål.
- Informationssäkerhetsarbetet ska främja verksamheternas funktionalitet, kvalitet och effektivitet samt invånares rättigheter och personliga integritet. Arbetet ska också främja Region Blekinges förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för informationshantering och IT-system.
- Informationssäkerhetsarbetet ska stödja Region Blekinges ledning så att underlag för uppföljning och prioritering finns.
- Det systematiska och riskbaserade arbetet med informationssäkerhet, sker enligt etablerade standarder med utgångspunkt i SS-ISO/IEC 27001, som är införd i verksamheten genom Region Blekinges ledningssystem.

Dataskydd

- Målet för dataskyddsarbetet är att säkerställa individers personliga integritet vid behandling av deras personuppgifter inom Region Blekinges verksamhet.
- Dataskyddsarbetet ska vara riskbaserat och utgå ifrån personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål och vilka risker som finns för individers rättigheter och friheter.
- Organisatoriska och tekniska åtgärder ska utformas så att de säkerställer ett adekvat skydd i enlighet med tillämplig dataskyddslagstiftning.

Innebörd

Informationssäkerhet

Informationssäkerheten är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder för att skydda informationen mot de hot den kan utsättas för. Informationssäkerhetsarbetet utgår från verksamhetens, lagars och föreskrifters krav utifrån nedanstående fyra perspektiv.

- Tillgänglighet – informationen ska finnas till hands när den behövs och där den behövs.
- Konfidentialitet – informationen ska bara vara åtkomlig för den som har rätt att ta del av den och på ett sådant sätt att den personliga integriteten eller sekretessen inte hotas.
- Riktighet – informationen måste vara korrekt, begriplig och fullständig. Den får inte förändras eller gå förlorad, av misstag, på grund av obehöriga eller som ett resultat av tekniska problem.
- Spårbarhet – att man i efterhand kan identifiera vem som gjort vad och när det har skett.

Principerna ska omfatta all information och alla it-system verksamhet inklusive medicinteknik och industriella informations- och styrsystem. Region Blekinges krav på informationssäkerhet är konkretiserad i dokumentet Regler för informationssäkerhet.

Personuppgiftsbehandling

Varje behandling ska ske med hänsyn till den enskildes personliga integritet och rättigheter samt i enlighet med gällande lagstiftning. Nedanstående principer enligt Dataskyddsförordningen (EU) 2016/679, artikel 5 ska följas:

- *Laglighet, korrekthet och öppenhet* - Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
- *Ändamålsbegränsning* - Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Behandling som inte ryms inom det ursprungliga ändamålet är inte tillåtet.
- *Uppgiftsminimering* - Uppgifterna ska vara adekvata, relevanta och inte omfatta fler personuppgifter än vad som är nödvändigt.
- *Riktighet* – Uppgifterna ska vara riktiga och om nödvändigt uppdaterade.
- *Lagringsminimering* – uppgifterna får inte lagras under en längre tid än vad som är nödvändigt för de ändamål som de samlats in för.
- *Integritet och konfidentialitet* - Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet med användning av tekniska eller organisatoriska åtgärder.
- *Ansvarsskyldighet* - Den personuppgiftsansvarige ska ansvara för och kunna visa att behandling sker i enlighet med principerna.

Utöver ovanstående principer ska de registrerade informeras om sin personuppgiftsbehandling på ett lättillgängligt sätt. Informationen ska även omfatta den registrerades rättigheter.

Behandlingen av personuppgifter i Region Blekinge är konkretiserad i dokumentet Riktlinjer – Principer för behandling av personuppgifter.

Genomförande

Skyddsåtgärder

Region Blekinge ska beskriva och införa organisatoriska, administrativa och tekniska skyddsåtgärder som är nödvändiga för att säkerställa en tillräcklig informationssäkerhet. Åtgärderna 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 (informationsklassning) och de konsekvenser som bristande säkerhet och tillgänglighet kan innebära för alla intressenter av 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.

Personuppgiftsbehandling

För Region Blekinge ska kunna ta sitt ansvar som personuppgiftsansvarig enligt Dataskyddsförordningen EU) 2016/679 ska dataskyddsarbetet organiseras på ett sådant sätt att verksamheten har möjlighet att uppfylla målen för dataskydd.

Ansvar

- Regionfullmäktige fastställer policy för informationssäkerhet och dataskydd

- Regionstyrelsen ger Regiondirektören i uppdrag att ansvara för omfattning och inriktning av informationssäkerhets- och dataskyddsarbetet. Detta sker genom fastställande av organisation, regler och riktlinjer.

- Ansvaret för informationssäkerheten och behandlingen av personuppgifter ska vara kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för informationssäkerhet och behandling av personuppgifter inom sin verksamhet.

- Den som ingår avtal som innefattar informationsutbyte och behandling av personuppgifter ansvarar för att kraven på informationssäkerhet specificeras i avtalet samt att personuppgiftsbiträdesavtal skrivs.

- Varje anställd ansvarar för att följa informationssäkerhetsregler och att rapportera fel och störningar i informationssystem, utrustningar och informationsinnehåll enligt fastställda rutiner. De ansvarar också för att behandla personuppgifter enligt med gällande lagstiftning och enligt regionen riktlinjer och rutiner.

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

Beslut om undantag enligt HSLF-FS 2016:40

Region Blekinge beslutar att göra ett undantag enligt HSLF-FS 2016:40 3 kap. § 16 genom att tillåta att påminnelser och kallelser till vård och behandling i enlighet med 3 kap. 17 § kan överföras via öppna nät t.ex. med sms.

Hantering av incidenter

Det ska finnas en formellt fastlagd rutin för rapportering och uppföljning av informationssäkerhets-incidenter.

Uppföljning och revidering

Följsamheten till denna policy, riktlinjer och regelverk ska regelbundet följa upp. Dataskyddsombud och informationssäkerhetsstrateg ska regelbundet rapportera läge och status tillhögsta ledningen.

Uppföljning och revidering av denna policy ska ske regelbundet vid ledningens genomgång. I samband med revidering ska tillhörande riktlinjer och instruktioner samt handlingsplanen för informationssäkerhet revideras på motsvarande sätt.

Denna policy ersätter nuvarande Policy för informationssäkerhet (dnr 2015/00256).