Dokumenttyp	Ansvarig verksamhet	Revision	Antal sidor
Policy	HS stab - informationssäkerhetsfunktionen	1.0	4
Dokumentägare	**Fastställare**	**Giltig fr.o.m.**	**Giltig t.o.m.**
Eije Berneflo	Landstingsfullmäktige	2012-11-28	2018-12-31

Informationssäkerhetspolicy

Gäller för: Landstinget i Värmland

Fastställd av landstingsfullmäktige 2012-11-28 LK/121686

Innehållsförteckning

1. Bakgrund, informationssäkerhet

Verksamheten inom Landstinget i Värmland grundas på principer om öppenhet, personlig integritet och respekt för individen. Medborgarna ska ha insyn i landstingets verksamhet. De ska kunna lita på den information som landstinget lämnar och vara förvissade om att den information som samlas in får ett tillräckligt skydd.

Information är en av landstingets strategiska resurser.

Alla landstingets verksamheter är beroende av tillförlitlig information. Avbrott i tillgången till information kan vara kritiskt för verksamheten och felaktig information kan bokstavligen vara livsfarlig inom hälso- och sjukvård.

Allt mer komplexa system hanterar känsliga uppgifter om medborgares medicinska, sociala och andra personliga förhållanden. De möjliggör effektivisering av verksamheten och därmed bättre service till medborgarna.

Beroendet av informationssystem medför sårbarhet om inte säkerheten beaktas. Det är därför nödvändigt att ställa säkerhetskrav utifrån ett verksamhetsperspektiv. Kraven ska ställas inför upphandling, utveckling, användning och avveckling av informationssystem och fortlöpande följas upp.

Arbetet med informationssäkerhet måste vara medvetet och strukturerat med tydliga mål och riktlinjer. Denna policy beskriver de övergripande principer som ska gälla för informationssäkerheten inom Landstinget i Värmland.

2. Mål

Målet för landstingets informationssäkerhetsarbete är att skydda informationstillgångarna så att verksamheten samtidigt har hög säkerhet och god tillgång till informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för landstingets verksamheter att uppnå sina mål.

3. Omfattning

Informationssäkerhetspolicyn gäller för hanteringen av information oavsett bärare inom landstinget. Policyn inkluderar samtliga externa handhavare som arbetar på uppdrag av landstinget. De sistnämnda regleras genom avtal.

4. Innebörd

Informationssäkerhet är den samlade effekten av de administrativa och tekniska åtgärder som vidtas för att skydda information mot de hot som den kan utsättas för. Följande skyddsaspekter ska beaktas.

Konfidentialitet (rätt person)

Information får inte göras tillgänglig eller avslöjas på ett sådant sätt att den personliga integriteten eller sekretessen hotas.

Riktighet (rätt information)

Informationen får inte förändras eller gå förlorad, vare sig genom misstag, inverkan av obehörig eller tekniskt fel.

Tillgänglighet (rätt tid och plats)

Informationen ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats.

Spårbarhet (uppföljning och kontroll)

Aktiviteter i systemen ska alltid kunna spåras.

5. Skyddsåtgärder

Skyddsåtgärder ska baseras på informationens betydelse för verksamheten och de konsekvenser som bristande säkerhet kan medföra. Informationens betydelse värderas genom informationsklassning. Åtgärderna följs upp genom riskanalyser.

Krav i lagar och förordningar utgör den lägsta nivå som ska uppnås med säkerhetsåtgärderna. Åtgärderna ska dokumenteras på ett sådant sätt att det blir möjligt att kontrollera att rätt skyddsnivå uppnås.

En förutsättning för arbetet med informationssäkerhet är att en god säkerhetskultur genomsyrar organisationen. Med detta menas inte bara att medarbetarna har god kunskap om vilka säkerhetsregler som gäller utan att de också har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka säkerheten.

Landstinget ska arbeta med planering som säkerställer verksamhetens kontinuitet. Kritiska verksamheter ska kunna upprätthållas vid katastrofsituation, störning eller avbrott.

6. Ansvar

Landstingsfullmäktige fastställer landstingets informationssäkerhetspolicy.

Informationssäkerhetsarbetet ska bedrivas i enlighet med patientdatalagen, offentlighets- och sekretesslagen, personuppgiftlagen, Socialstyrelsens föreskrifter, svensk standard SS-ISO/IEC 27000 samt strategi och handlingsplan för samhällets informationssäkerhet från Myndigheten för samhällsskydd och beredskap (MSB).

Landstingsstyrelsen ansvarar

- för att landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella
- för samordningen av informationssäkerhetsarbetet i landstinget och ska därför årligen fastställa en handlingsplan för informationssäkerhetsarbetet
- för att det utses en person som ansvarar för landstingets informationssäkerhetsarbete

Ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret i linjeorganisationen. Det betyder att *varje verksamhetschef* är ansvarig för informationssäkerheten inom sin verksamhet.

Varje anställd ansvarar för att säkerhetsregler följs samt att störningar och fel i informationssystem, utrustning och informationsinnehåll rapporteras enligt fastställda rutiner.

7. Uppföljning

Denna policy ska följas upp regelbundet.

Landstingets informationssäkerhetsarbete ska rapporteras till landstingsstyrelsen minst en gång per år.

8. Revidering

Denna policy ska revideras vart tredje år. I samband med revidering ska handlingsplanen för informationssäkerhet revideras på motsvarande sätt.

Utarbetad av: Strategisk grupp för informationssäkerhet, informationssäkerhetsansvarig Eije Berneflo.