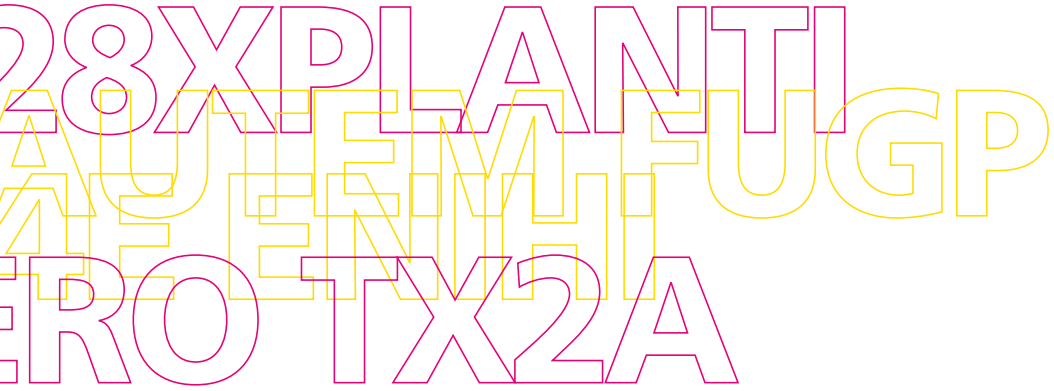
Informationssäkerhetspolicy för Stockholms läns landsting

Stockholms läns landsting



Innehållsförteckning

LS 1112-1733
Beslutad av landstingsfullmäktige 2013-03-19
Informationsklass: K1R2Ti

LSF Kommunikation
Grafisk form: Fidelity Stockholm, september 2014.


Foto Fredrik Hjerling

Inledning

Stockholms läns landstings verksamhet är grundad på principer om öppenhet, personlig integritet och respekt för individen. Medborgarna ska kunna få insyn i landstingets verksamhet. De ska kunna förlita sig på den information som landstinget lämnar och vara förvissade om att information som samlas in får ett tillräckligt skydd.

Information är en av landstingets mest strategiska resurser. Alla verksamheter är beroende av tillförlitlig information. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser inom hälso- och sjukvården, kollektivtrafiken och inom landstingets övriga ansvarsområden.

Utvecklingen med informationshantering i IT-system och nya funktionaliteter innebär förbättringar i många avseenden. Samtidigt innebär beroendet av informationssystem att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas.

Därför arbetar Stockholms läns landsting aktivt med informationssäkerhet. Det innebär att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta, och att obehöriga inte får åtkomst till dem. Genom att arbeta systematiskt och långsiktigt upprätthåller vi ett tillräckligt skydd som är anpassat efter våra verksamheters förutsättningar och behov.

Informationssäkerhetsarbetet syftar till att stödja och säkerställa landstingets verksamhet. Alla medarbetare deltar i detta arbete. Informationssäkerhetsarbetet är en viktig del i landstingets övergripande arbete med intern styrning och kontroll samt riskhantering.

Denna policy beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Stockholms läns landsting.


Foto: Maskot

Mål

Målet för landstingets informationssäkerhetsarbete är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för landstingets verksamheter att uppnå sina mål.

En god informationssäkerhet inom landstinget främjar verksamheternas funktionalitet, kvalitet och effektivitet, medborgares rättigheter och personliga integritet, landstingets förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för landstingets informationshantering och IT-system.

Omfattning

Informationssäkerhetspolicyn gäller för hantering av information, i alla dess former, i Stockholms läns landsting inklusive bolag och stiftelser och av samtliga som arbetar på uppdrag av landstinget. Det sistnämnda regleras genom avtal.

Informationssäkerhetsarbetet styrs med hjälp av landstingets ledningssystem för informationssäkerhet som är framtaget med stöd av standarden för informationssäkerhet, ISO/IEC 27000 och utifrån organisationens verksamhetskrav samt gällande lagar och föreskrifter.

Vårt ledningssystem är uppbyggt i två nivåer. Nivåerna ger en struktur för ledning och styrning av informationssäkerheten på både övergripande nivå och på verksamhetsnivå. En viktig del av ledningssystemet är regelverket. Det består av styrande dokument som på övergripande nivå utgörs av denna policy och tillhörande riktlinjer och tillämpningsanvisningar. Allt informationssäkerhetsarbete utgår från dessa dokument.

Respektive nämnd, styrelse och bolag styr och leder sitt informationssäkerhetsarbete i ett lokalt ledningssystem inom dess verksamhetsområde. Det innehåller de nödvändiga processer och rutiner som behövs för att säkerställa att verksamheten uppfyller kraven på en ändamålsenlig informationssäkerhet. De styrande dokumenten på lokal nivå utformas utifrån de övergripande.

Utöver detta krävs att Stockholms läns landsting i tillämpliga delar lever upp till gällande lagar och förordningar samt till landstingets övriga styrande dokument.

Innebörd

Informationssäkerhetsarbetet innebär att värdera all information efter sin känslighet och med hjälp av administrativa och tekniska skyddsåtgärder säkerställa att den finns tillgänglig när den behövs, att den är korrekt och

att obehöriga inte kan få tillgång till den. Utöver dessa säkerhetsaspekter måste behov av spårbarhet uppfyllas – att i efterhand kunna avgöra vem som tagit del av informationen, vilka förändringar som skett och av vem dessa utförts.

Säkerhetsaspekter

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, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.

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

Spårbarhet:
Händelser i informationsbehandlingen ska kunna spåras.

Skyddet av informationstillgångar och informationssystem ska vara utformat så att verksamhetens krav på dessa säkerhetsaspekter uppfylls. Detta gäller även när landstingets information eller informationssystem hanteras av extern part.

Skyddsåtgärder

För att hitta relevant skyddsnivå utifrån dessa fyra aspekter ska vi arbeta utifrån nedanstående principer:

- Vi ska arbeta med informationsklassificering där all information klassificeras och handlingar och dokument märks.
- All information ska ha en ägare. Informationsägaren ansvarar för att klassificera informationen och ställa de säkerhetskrav som krävs för informationshantering.
- Alla informationssystem ska ha en systemägare som ansvarar för att säkerhetskraven på systemet uppfylls.
- Omvärlden förändras. Därför ska vi, utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder för att se till att vår information har rätt skydd.
- Vi ska ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationssystem och vi ska följa upp de krav vi ställt.
- Vi ska arbeta med kontinuitetsplanering och ha beredskap för avbrott. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av katastrofsituationer, störningar och avbrott.
- Alla anställda ska veta vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas.
- Det är viktigt att alla har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.
- Skyddsåtgärder skall vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.
- Kontinuerlig uppföljning ska ske mot fastställda regler.

Ansvar

Landstingsfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för landstinget.

Landstingsstyrelsen ansvarar för att landstingets informationssäkerhetspolicy och riktlinjer för informationssäkerheten utarbetas och hålls aktuella. Landstingsstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i landstinget och ska därför årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Landstingsdirektören har landstingstingsstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt. Landstingsdirektören ansvarar för att övergripande tillämpningsanvisningar utarbetas och hålls aktuella i enlighet med policy och riktlinjer.

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

Varje nämnd och styrelse är ansvarig för informationssäkerheten inom sitt verksamhetsområde och ska därför, inom ramen för

sitt lokala ledningssystem och i enlighet med tillämpningsanvisningar, anta verksamhetsnära styrdokument för informationssäkerhet. Det åligger även varje nämnd och styrelse att årligen planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret.

Förvaltningschef/VD ska säkerställa att all informationshantering inom den egna verksamheten sker i enlighet med denna policy samt tillhörande riktlinjer och tillämpningsanvisningar för informationssäkerhet.

Informationssäkerhetssamordnare ska utses inom varje förvaltning och bolag och ges i ansvar att samordna och följa upp det för organisationen och verksamheten gemensamma informationssäkerhetsarbetet.

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

Informationssäkerhetsrådets uppgift är att främja, stödja, samordna och följa upp landstingets informationssäkerhetsarbete på en övergripande nivå.

Landstingsrevisorernas uppgift är att granska om den interna kontrollen är tillräcklig.

Uppföljning och revidering

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


Foto: Maskot