Stockholms läns landsting

Landstingsrådsberedningen

SKRIVELSE
2016-02-10

LS 1308-1044

Landstingsstyrelsen

Handlingsprogram för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

I tjänsteutlåtandet ges förslag på handlingsprogram för informationssäkerhet för åren 2016-2020 och för Stockholms läns landsting i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området.

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att anta Handlingsprogram för informationssäkerhet för åren 2016-2020 enligt förslag

att uppdra åt landstingsdirektören att besluta om ändringar av eller tillägg till Handlingsprogram för informationssäkerhet 2016-2020 som gäller den verksamhetsspecifika delen av programmet.

Landstingsrådsberedningens motivering

Den höga förändringstakten inom Stockholms läns landsting och genomförandet av framtidsplanen ställer höga krav på informationshantering och informationssäkerhet. Handlingsprogrammet är det första gemensamma programmet för informationssäkerhet för landstingets verksamheter. Det höjer ambitionsnivån och anger grundläggande målsättningar och arbetssätt. Med ett fokuserat och systematiskt arbete med informationssäkerhet, som utvecklas i takt med omvärlden, ska landstinget vara väl förberett i händelse av en kris eller annan allvarlig händelse i syfte att minska de negativa konsekvenserna för invånarna i länet.

Ett ökat fokus på informationssäkerhet är också avgörande för landstingets arbete med att garantera högsta möjliga skydd av känslig information och skydd av den personliga integriteten. För att öka landstingets medarbetares säkerhetsmedvetande och ansvar som användare av vårdens IT-system ska all personal genomgå grundläggande informationssäkerhetsutbildning.

I handlingsprogrammet finns fyra målområden och elva landstingsgemensamma inriktningsmål för informationssäkerhet. Uppföljning och återrapportering om programmets genomförande kommer att ske årligen till landstingsdirektören och till landstingsstyrelsen. De verksamhetsspecifika målen ska vara uppnådda innan programperiodens slut 2020.

Beslutsunderlag

Arbetsutskottets protokollsutdrag den 26 januari 2016
Innovationsberedningens protokollsutdrag 18 januari 2016
Landstingsdirektörens tjänsteutlåtande den 29 december 2015
Handlingsprogram för informationssäkerhet för åren 2016-2020

Torbjörn Rosdahl

Daniel Forslund

Carl Rydingstam

§ 9
Handlingsprogram för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området

LS 1308-1044

Ärendebeskrivning

I tjänsteutlåtandet ges förslag på handlingsprogram för informationssäkerhet för åren 2016-2020 och för Stockholms läns landsting i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 29 december 2015
Handlingsprogram för informationssäkerhet för åren 2016-2020
Protokollsutdrag från Innovationsberedningen 18 januari 2016

Arbetsutskottets beslut

Arbetsutskottet beslutar föreslå landstingsstyrelsen besluta

att anta Handlingsprogram för informationssäkerhet för åren 2016-2020

att uppdra åt landstingsdirektören att besluta om ändringar av eller tillägg till Handlingsprogram för informationssäkerhet 2016-2020 som gäller den verksamhetsspecifika delen av programmet.

Beslutsexpediering:
Landstingsstyrelsen
Akt

§ 2

Handlingsprogram för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området

LS 1308-1044

Ärendebeskrivning

I tjänsteutlåtandet ges förslag på handlingsprogram för informationssäkerhet för åren 2016-2020 och för Stockholms läns landsting i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 29 december 2015
Handlingsprogram för informationssäkerhet för åren 2016-2020

Förslag och yrkande

Ordförandens förslag om bifall till landstingsdirektörens förslag.

Innovationsberedningens beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att anta Handlingsprogram för informationssäkerhet för åren 2016-2020 enligt förslag

att uppdra åt landstingsdirektören att besluta om ändringar av eller tillägg till Handlingsprogram för informationssäkerhet 2016-2020 som gäller den verksamhetsspecifika delen av programmet.

Beslutsexpediering:
Arbetsutskottet
Akt

Landstingsstyrelsens förvaltning
Direktör strategisk IT i SLL
SLL Informationssäkerhet

Handläggare:
Vesna Lucassi

TJÄNSTEUTLÅTANDE
2015-12-29

LS 1308-1044
Ankom
Stockholms läns landsting
2016 -01- 04
Dnr LS 1308-1044

Landstingsstyrelsens
innovationsberedning

Handlingsprogram för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området

Ärendebeskrivning

I tjänsteutlåtandet ges förslag på handlingsprogram för informationssäkerhet för åren 2016-2020 och för Stockholms läns landsting i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 29 december 2015
Handlingsprogram för informationssäkerhet för åren 2016-2020

Förslag till beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att anta Handlingsprogram för informationssäkerhet för åren 2016-2020 enligt förslag

att uppdra åt landstingsdirektören att besluta om ändringar av eller tillägg till Handlingsprogram för informationssäkerhet 2016-2020 som gäller den verksamhetsspecifika delen av programmet.

Förvaltningens förslag och motivering

Sammanfattning
Ärendet gäller förslag på handlingsprogram för informationssäkerhet för Stockholms läns landsting. Det är landstingets första gemensamma program inom området och har en programperiod som sträcker sig till år 2020. Genom föreslaget handlingsprogram höjs ambitionsnivån för informationssäkerhetsarbetet inom landstinget.

Bakgrund
I Mål och budget för år 2014 som beslutades i Stockholms läns landstingsfullmäktige i juni 2013, gavs landstingsstyrelsen i uppdrag att utarbeta ett handlingsprogram för informationssäkerhet i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området, LS 1301-0040, sid. 176.

Överväganden
Stockholms läns landsting står inför en stor förändringsprocess. För att möta framtidens behov genomför landstinget just nu en av de största satsningarna någonsin inom vård och trafik. Genomförandet av framtidsplanerna kräver en hög förändringstakt, vilket i sin tur kommer att ställa högre krav på informationshantering och informationssäkerhet inom landstinget. Samtidigt ställer en stark utveckling av informationssäkerhetsfrågorna i samhället i allmänhet ökande krav på landstingets förmåga inom området.

Handlingsprogrammet består av två delar. Den ena delen utgörs av en övergripande programdel med inriktningsmål som föreslås beslutas av landstingsstyrelsen. Landstingsstyrelsen antar i detta handlingsprogram fyra målområden och elva landstingsgemensamma inriktningsmål för informationssäkerhet. Uppföljning av dessa mål ska göras i samband med återrapportering till landstingsstyrelsen.

Den andra delen utgörs av en verksamhetsspecifik del med övergripande och tidssatta mål och indikatorer. Med hänsyn till att denna del kan behöva revideras och uppdateras föreslås landstingsstyrelsen delegera beslutskompetens till landstingsdirektören som bemyndigas att i sin tur vidaredelegera beslutanderätten till den han utser. Avsikten är att genomföra justeringar för att få en bättre och mer heltäckande bild av arbetet för att nå inriktningsmålen och av utvecklingen. Beslut om revidering av handlingsprogrammet som fattas med stöd av denna delegation ska anmälas till landstingsstyrelsen. Beslutsmandatet inkluderar

inte sådana ändringar eller tillägg som kan sägas påverka verksamhetens mål, inriktning, omfattning eller kvalitet (6 kap 34§ kommunallagen).

De verksamhetsspecifika målen ska vara uppnådda innan programperiodens slut 2020. Föreslagna indikatorerna är valda för att få ett grepp om i vilken riktning utvecklingen går och ge en översiktlig bild av eventuella behov av att utveckla styrning och ledning av området.

Handlingsprogrammet är ett verktyg för förvaltningars och bolags informationssäkerhetsarbete. För att förverkliga programmets intentioner behöver målen brytas ner ytterligare och konkretiseras med delmål och åtgärder. Detta görs genom förvaltningars och bolags lokala handlingsplaner.

Genom föreslaget handlingsprogram höjs ambitionsnivån för informationssäkerhetsarbetet inom landstinget. Programmets genomförande ska följas upp och rapporteras årligen till landstingsdirektören och till landstingsstyrelsen.

Handlingsprogrammet har arbetats fram i samråd med landstingets informationssäkerhetsråd, ISR, med representanter från förvaltningars och bolags informationssäkerhetssamordnare. Programmet har även samberetts med utvalda representanter från landstingets olika verksamheter, bland annat ansvariga för it-verksamheter, chefläkare, personuppgiftsombud och jurister. Inkomna synpunkter har behandlats och beaktats.

Ekonomiska konsekvenser av beslutet

Landstingsstyrelsen och fullmäktige beslutade i mars 2013 om en ny informationssäkerhetspolicy och nya riktlinjer för informationssäkerhetsarbetet inom Stockholms läns landsting. Dessa ska efterlevas av samtliga nämnder, styrelse och bolag inom landstinget och av samtliga som arbetar på uppdrag av landstinget. Det sistnämnda regleras genom avtal. Landstingets samtliga verksamheter ska vidta skyddsåtgärder för att uppnå och vidmakthålla eftersträvad nivå på informationssäkerheten.

Kostnaderna för genomförandet av handlingsprogrammet ska rymmas inom respektive verksamhets budget. Innehållet i handlingsprogrammet motsvarar krav som redan ställs på landstingets verksamheter liksom redan beslutade åtgärder.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Toivo Heinsoo
Landstingsdirektör

Anders Nyström
Direktör strategisk IT i SLL

Stockholms läns landsting

HANDLINGSPROGRAM

Diarienummer
LS 1308-1044

Stockholms läns landsting

Handlingsprogram för informationssäkerhet 2016-2020

Dokumenttyp Viljeriktning	Fastställd	Giltig till och med 2020-12-31
Dokumentnummer	Fastställd av	Upprättad av Informationssäkerhetschef
Informationssäkerhetsklass K1R2T2	Verksamhetstyp	

Innehållsförteckning

1. Inledning 3

2. Handlingsprogrammets struktur och målgrupp 5

3. Landstingets inriktningsmål för informationssäkerhet 8

4. Målområde 1: Information 9

5. Målområde 5: Medarbetare 10

6. Målområde 3: Processer 12

7. Målområde 4: It-säkerhet 14

8. Styrmedel - så når landstinget målen 16

9. Nationella strategier och handlingsplaner för informationssäkerhet 18

10. Referenser 19

1. Inledning

1.1 Om Stockholms läns landsting

Stockholms läns landstings främsta uppgift är att se till att länets invånare har tillgång till en bra och väl fungerande hälso- och sjukvård samt kollektivtrafik. Stockholms läns landsting ansvarar även för regionplanering och för att bidra till ett fritt och tillgängligt kulturliv i länet. Landstinget har ett regionalt sektorsansvar för hälso- och sjukvård, smittskydd, kollektivtrafik och tandvård.

1.2 Ett landsting i förändring

Landstinget står inför en stor förändringsprocess. Mellan åren 2010 och 2020 beräknas befolkningen i Stockholms län öka med 350 000 personer. För att möta framtidens vårdbehov genomför landstinget just nu en av de största satsningarna någonsin inom hälso- och sjukvården. Totalt 42 miljarder kronor ska resultera i mer vård, bättre lokaler och nya arbetsmetoder. Utvecklingen pekar mot en ökad rörlighet för såväl patienter som anställda. Vården ska fortsätta att utvecklas mot mer vård i hemmet och mer öppenvård.

Det regionala trafikförsörjningsprogrammet och den regionala utvecklingsplanen rymmer ambitionerna för att möta de utmaningar som den växande Stockholmsregionen står inför. Dessa består i att vårda och utveckla befintlig infrastruktur, att genomföra en kraftigt utbyggnad av tunnelbanan och att skapa förutsättningar för en växande och fungerande Stockholmsregion.

Framtidsplanerna omfattar även satsningar på e-hälsa och IT. Den höga förändringstakten inom landstinget och det ökande behovet av informationsdelning ställer samtidigt också högre krav på informationshantering och informationssäkerhet.

1.3 Systematiskt informationssäkerhetsarbete

En förutsättning för att landstinget ska kunna nå sina målbilder är att vi arbetar med informationssäkerhet på ett fokuserat och systematiskt sätt. Mycket görs redan idag, men det krävs mer. Landstingets arbete med informationssäkerhet behöver ständigt utvecklas i takt med omvärlden. Likaså behöver landstingets förvaltningar och bolag anpassa sitt informationssäkerhetsarbete till de nya arbetssätten utifrån visionen och målen i våra styrande framtidsplaner.

Hälso- och sjukvård och kollektivtrafik är samhällsviktiga verksamheter. Detta innebär att landstinget har ett särskilt ansvar att arbeta på ett

systematiskt sätt för att skydda och säkerställa funktionalitet och kontinuitet i sådana verksamheter. En stark utveckling av informationssäkerhetsfrågorna i samhället ställer ökande krav på landstingets förmåga inom området.

1.4 Landstingets första handlingsprogram för informationssäkerhet

Detta är vårt första gemensamma handlingsprogram för informationssäkerhet. Det konkretiserar färdriktningen och anger grundläggande målsättningar och arbetssätt för informationssäkerhet inom Stockholms läns landsting. För att det som står i programmet ska bli verklighet behöver alla hjälpas åt. Vissa mål berör förvaltningar och bolag, medan andra berör it-verksamhet specifikt. Ansvaret för att nå målen i handlingsprogrammet ligger i den ordinarie linjeorganisationen.

Handlingsprogrammet är ett verktyg för förvaltningars och bolags informationssäkerhetsarbete. För att förverkliga programmets intentioner behöver målen brytas ner ytterligare och konkretiseras med delmål och åtgärder. Detta görs genom förvaltningars och bolags lokala handlingsplaner.

Den övergripande visionen är långsiktig. Informationssäkerhetspolicyn visar de grundläggande utgångspunkterna för hur landstinget ska arbeta för att uppnå visionen.

Handlingsprogrammet består av två delar: en övergripande programdel med inriktningsmål som beslutas av landstingsstyrelsen och en verksamhetsspecifik del med övergripande och tidssatta effektmål och resultatmål som beslutas av landstingsdirektören.

Programmet har utformats som en pågående satsning över tid som kommer att förändras genom en revidering av strategi och inriktning i slutet av varje programperiod. De åtgärder som beskrivs i handlingsprogrammet kommer att kunna genomföras inom befintliga budgetramar. Framtida åtgärder kan komma att kräva ytterligare resurser.

Eftersom vi förväntar oss att det kommer att ske förändringar under programtiden är det viktigt med en årlig uppföljning av den verksamhetsspecifika delen. Den kan därför komma att behöva revideras för att hållas aktuell.

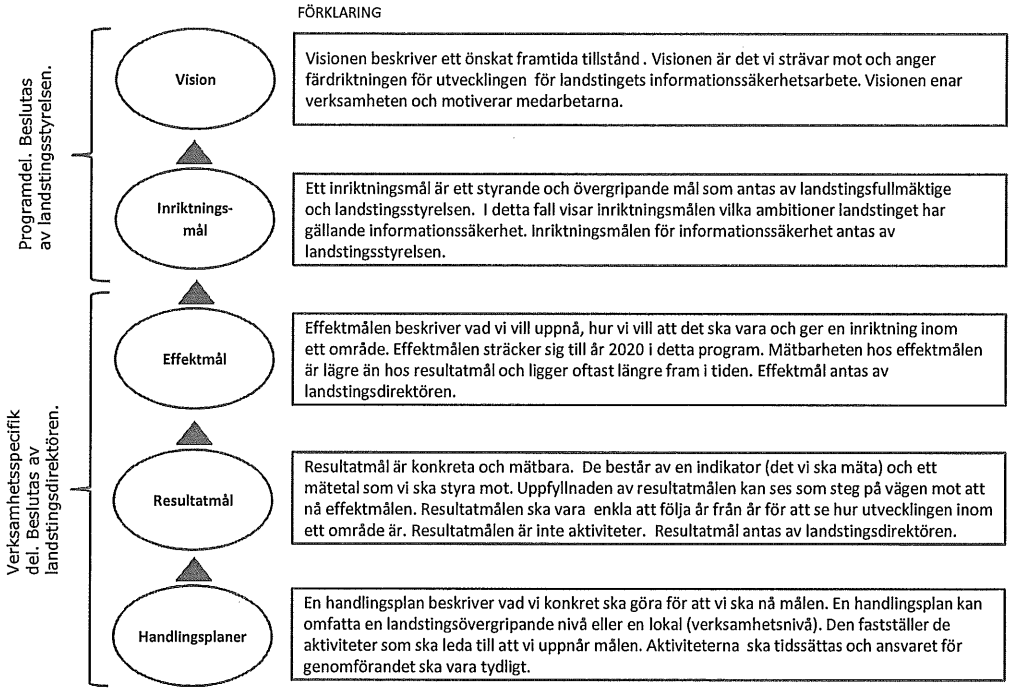
2. Handlingsprogrammets struktur och målgrupp

1.5 Styrmodell

Budgeten som beslutas av fullmäktige är landstingets viktigaste styrdokument och beskriver mål, satsningar, ekonomiska ramar samt anger inriktning för vad landstingets verksamheter ska uppnå[1].

Inriktningen för vårt informationssäkerhetsarbete beskrivs närmare i informationssäkerhetspolicyn[2].

Handlingsprogrammets styrmodell utgörs av målstyrning med följande styrstruktur:



1.6 Målgrupp

Målgrupp för handlingsprogrammet är främst informationssäkerhets-samordnare samt chefer med verksamhetsansvar som har i uppgift att säkerställa informationssäkerheten i landstingets verksamheter.

---

[1] Mål och budget 2016, LS 2015-0039, LS 1312-1542.
[2] Informationssäkerhetspolicy för Stockholms läns landsting, LS 1112-1733.

1.7 Stockholms läns landstings vision och mål

Stockholmsregionen ska bli Europas mest attraktiva storstadsregion. Det är en vision som kommuner, landsting, myndigheter, näringsliv, högskolor och universitet samt intresseorganisationer i regionen har kommit överens om i den regionala utvecklingsplanen för Stockholmsregionen, RUFS 2010.

Budgeten är landstingets viktigaste styrande dokument och beskriver landstingets mål och ekonomiska ramar. Den anger också inriktning för landstingets verksamheter. Landstinget har sex övergripande mål som fördelas på arton nedbrutna mål och följs upp med indikatorer.

Ett av de övergripande målen är Hållbar tillväxt. Det i sin tur har fyra nedbrutna mål varav ett är Säkra processer. Det anger att säkerhetsarbetet ska bedrivas på ett systematiskt sätt. Uppföljning sker i samband med bokslut och mätning sker med hjälp av en övergripande indikator för landstingets informationssäkerhetsarbete: andel förvaltningar och bolag som har infört metoder och verktyg för ett systematiskt arbete. I årsredovisningarna ska man kunna läsa om hur förvaltningar och bolag har lyckats uppfylla målet.

Delmålet Säkra processer innebär att landstingets processer ska vara kvalitetssäkrade hela vägen från planering och genomförande till uppföljning och åtgärder. Den snabba it-utvecklingen, komplexa system och ökad informationsdelning kräver säkra processer för informationshantering. Landstinget ska också vara väl förberett i händelse av en kris eller annan allvarlig händelse i syfte att minska de negativa konsekvenserna för invånarna i länet.

1.8 Informationssäkerhetspolicy

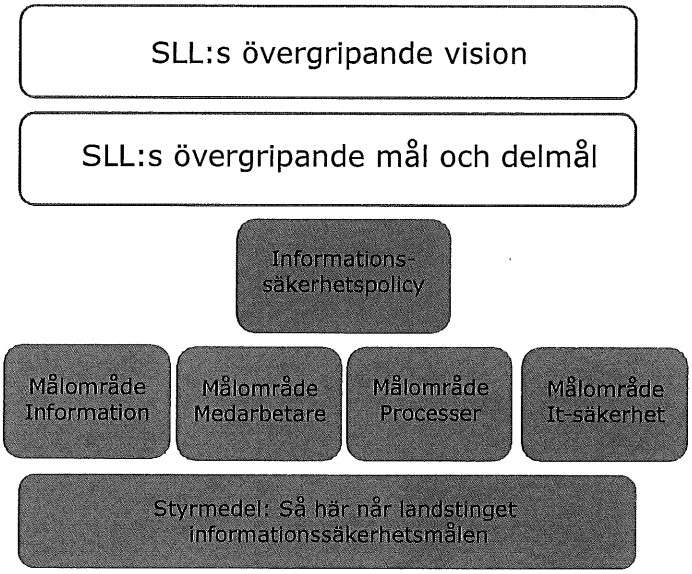
Informationssäkerhetspolicyn anger inriktningen för landstingets informationssäkerhetsarbete. Målet är att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav och därigenom möjliggöra för landstingets verksamheter att uppnå sina mål.

1.9 Målområden, mål och indikatorer

Landstinget ska utföra sitt uppdrag på ett sätt som är informationssäkert. Detta innebär säker informationshantering, säkerhetsmedvetna medarbetare, säkra processer samt god it-säkerhet. Dessa utgör de fyra målområdena i handlingsprogrammet.

För varje målområde finns en långsiktig vision och flera inriktningsmål som sträcker sig förbi programperioden. Inriktningsmålen är övergripande och anger ett önskvärt framtida tillstånd. Inriktningsmålen översätts till flera verksamhetsspecifika mål - effektmål och resultatmål - som förvaltningar och bolag sedan genomför. Måluppfyllelsen följs upp i samband med bokslut och mätning sker med hjälp av ett flertal indikatorer.

Detta handlingsprogram tar sikte på att införa ett systematiskt arbete med informationssäkerhet, med fokus på uppbyggnad av ledningssystem för informationssäkerhet samt på start av egenkontroller i landstingets verksamhet. De verksamhetsspecifika målen ska vara uppnådda innan programperiodens slut 2020. Indikatorerna är valda för att få ett grepp om i vilken riktning utvecklingen går och ge en översiktlig bild av eventuella behov av att utveckla styrning och ledning av området. De kommer att utvärderas och utvecklas fortlöpande.



En del av målen i handlingsprogrammet är inte framtagna inom ramen för informationssäkerhetsarbetet. De är inlyfta från andra områden för att de har betydelse för och väsentligt bidrar till det systematiskt informations-säkerhetsarbetet.

3. Landstingets inriktningsmål för informationssäkerhet

Landstingsstyrelsen antar i detta handlingsprogram elva inriktningsmål för informationssäkerhet. Uppföljning av inriktningsmålen ska göras i samband med återrapportering till landstingsstyrelsen. De elva inriktningsmålen är:

Säker informationshantering

Stockholms läns landsting hanterar information utifrån dess skyddsbehov så att den är riktig och tillgänglig när den behövs.

Ansvarstagande organisation

Stockholms läns landsting tar ansvar för informationssäkerheten och har ett organisatoriskt ramverk som möjliggör ledning och styrning av informationssäkerhetsarbetet.

God säkerhetskultur

Behovet att skydda information bedöms på alla nivåer i verksamheten, och det finns en god kännedom om de risker och hot som finns mot informationen.

Behörig åtkomst

Information inom landstinget är åtkomlig för behöriga användare, och åtkomst styrs av lagstiftning och behov av tillgång till information.

Effektiv incidenthantering

Landstinget har en god förmåga att hantera och lära av allvarliga i informationssäkerhetsincidenter.

Kontinuitetsplanerade verksamheter (robusthet)

Landstingets verksamheter har planerat för vilka informationssäkerhetsåtgärder som ska vidtas vid avbrott eller störningar.

Skydd mot angrepp

Information och resurser för informationsbehandling inom landstinget skyddas mot skadlig kod och medarbetare är medvetna om sitt ansvar som användare av it-system.

Spårbarhet

Det är möjligt att härleda hur skyddsvärd information har hanterats inom landstinget.

Säker drift

Driftsatta it-system är riskbedömda och lever upp till kraven i styrande dokument för informationssäkerhet.

Säkra tjänster

Driftsatta tjänster är riskbedömda och lever upp till kraven i styrande dokument för informationssäkerhet.

Säker infrastruktur

Landstingets hårda och mjuka infrastruktur för informationsutbyte är riskbedömd och lever upp till kraven i styrande dokument för informationssäkerhet.

4. Målområde 1: Information

Vision
Stockholms läns landstings information hanteras säkert och effektivt och ger förutsättningar för en hälso- och sjukvård och kollektivtrafik som är effektiv och trygg för invånarna i länet.

Inriktningsmål
- Säker informationshantering

Effektmål 2020
- Landstingets information värderas genom informationsklassificering för att identifiera var skyddsbehov finns.
- Information hanteras på ett sådant sätt att obehörig åtkomst och obehörig förändring försvåras, samtidigt som en hög tillgänglighet upprätthålls.
- Informationshantering sker med de säkerhetsåtgärder som identifieras utifrån risk- och sårbarhetsbedömning samt styrande regelverk inom området.
- Landstingets verksamheter anpassar sitt informationssäkerhetsarbete till verksamheternas förändrade it-arbetssätt utifrån visionen och målen i de styrande framtidsplanerna, såsom Framtidsplan för hälso- och sjukvården, Trafikförsörjningsprogrammet etc.

Resultatmål 2020

Indikator	Del-mål 2017	Mål 2020
Andel förvaltningar och bolag som har informationssäkerhetsklassificerat minst hälften av sina informationstillgångar och därmed identifierar skyddsbehov för dessa.	50 %	90 %
Andel förvaltningar och bolag som genomför egenkontroller[3] av informations-säkerhet med verktyg för informationssäkerhet inom minst hälften av förvaltningens/bolagets olika verksamheter.	50 %	90 %
Andel SLL-gemensamma it-system vars ägarskap är utpekat.	50 %	90 %

[3] Med egenkontroll av informationssäkerhet menas kontroll i tre steg, d.v.s. deklaration, riskbedömning samt rapportering enligt landstingets s.k. compliance-process i nivå 2. Uppfyllandegrad ska anges.

5. Målområde 5: Medarbetare

Vision
Stockholm läns landstings medarbetare är säkerhetsmedvetna och ansvarstagande, och bidrar till förbättringar i ett öppet klimat.

Inriktningsmål
- Ansvarstagande organisation
- God säkerhetskultur

Effektmål 2020
- Informationssäkerhetsarbetet i landstingets verksamheter är en ledningsfråga och är kopplat till en tydlig beslutsordning i styrelser och nämnder.
- Landstingets verksamheter har förmåga att hantera informationssäkerhetsfrågor i enlighet med identifierat behov.
- Landstingets verksamhetschefer tar återkommande upp informationssäkerhet med medarbetare i syfte att skapa insikt om informationens värde och behov av skydd.
- Landstingets medarbetare är utbildad i informationssäkerhet i den omfattning som är relevant för befattningen.
- Medarbetare deltar aktivt i förbättringsarbetet genom att bland annat rapportera avvikelser och förbättringsförslag.

Resultatmål

Indikator	Del-mål 2017	Mål 2020
Andel förvaltningar och bolag som har fattat verksamhetsbeslut att införa ledningssystem för informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag som har fastställt organisation och processer för arbetet med informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag som har fastställt årlig handlingsplan för informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag som har genomfört ledningens genomgång av informationssäkerhet under året.	50 %	90 %
Andel förvaltningar och bolag som genomför egenkontroller[4] av den egna informationssäkerheten med verktyg för informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag där minst 50 % av medarbetarna har genomgått landstingets obligatoriska e-utbildning om informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag som har genomfört kartläggning och identifierat verksamhetens kompetensbehov inom informations-säkerhet.	50 %	90 %
Andel förvaltningar och bolag som under året har rapporterat informationssäkerhetsavvikelser i verktyg för avvikelsehantering.	50 %	90 %

[4] Med egenkontroll av informationssäkerhet menas kontroll i tre steg, dvs. deklaration, riskbedömning samt rapportering enligt landstingets s.k. compliance-process i nivå 1. Uppfyllandegrad ska anges.

6. Målområde 3: Processer

Vision
Stockholms läns landstings processer är kvalitetssäkrade och skapar effektivitet och stöd i landstingets verksamheter. Landstingets processer är robusta och har förmåga att motstå påfrestningar utan allvarliga brister i kontinuiteten.

Inriktningsmål
- Behörig åtkomst
- Effektiv incidenthantering
- Kontinuitetsplanerade verksamheter (robusthet)

Effektmål 2020
- Landstinget använder strukturerade processer för behörighetshantering och åtkomstbehov.
- Revision av behörigheter i it-system genomförs regelbundet.
- Landstingets funktion för upptäckt och hantering av it-säkerhets-relaterade hot och incidenter[5], SLL SOC, stödjer landstingets förvaltningar och bolag.
- Landstingets verksamheter har integrerat informationssäkerhet i sina kris-, kontinuitets- och beredskapsprocesser.
- Landstingets kritiska it-system är identifierade och kontinuitets-planerade.
- Landstingets verksamheter har en fastställd rutin för egenkontroll av informationssäkerhet i projektmodeller och upphandlingsprocesser.

[5] SLL SOC, Center för Incidentstöd inom it-säkerhet.

Resultatmål

Indikator	Del-mål 2017	Mål 2020
Andel it-system i förvaltningar och bolag med fastställda rutiner för behörighetshantering (tilldelning, borttagning och revision).	50%	90%
Andel förvaltningar och bolag som genomför årliga revisioner av behörigheter i it-system.	50%	90%
Andel förvaltningar och bolag som har säkerställt att deras processer för att hantera incidenter även omfattar informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag med it-drift som har etablerat kontaktyta med landstingets funktion för upptäckt och hantering av it-säkerhetsrelaterade hot och incidenter, SLL SOC.	75 %	90 %
Andel av förtecknade kritiska[6] it-system som har kontinuitetsplanerats.	25 %	75 %
Andel förvaltningar och bolag som följer landstingets projektmodell där krav finns att egenkontroller[7] av informationssäkerhet ska genomföras.	50 %	90 %
Andel förvaltningar och bolag som ställer informationssäkerhetskrav i upphandling så att levererade it-system och tjänster kan upprätthålla skyddsbehoven.	50 %	90 %

[6] Med kritiska it-system menas system som klassats T3 eller T4 enligt landstinget informationsklassificeringsmodell.

[7] Med egenkontroll av informationssäkerhet menas kontroll i tre steg, d.v.s. deklaration, riskbedömning samt rapportering enligt landstingets s.k. compliance-process.

7. Målområde 4: It-säkerhet

Vision
Stockholms läns landstings it-infrastruktur, it-system och elektroniska kommunikationer skapar verksamhetsnytta och är stabila, säkra och avbrottsfria.

Inriktningsmål
- Skydd mot angrepp
- Spårbarhet
- Säker drift
- Säkra tjänster
- Säker infrastruktur

Effektmål 2020
- Skydd mot skadlig kod inom landstinget är enhetligt uppsatt och rapporterar in misstänkta fall av skadlig kod till ett centralt system.
- Den personliga it-arbetsplatsen är standardiserad och skyddad.
- Landstinget har en säker hantering av intern utrustning som ansluts till landstingets nätverk.
- Landstinget har en säker hantering av extern utrustning som ansluts till landstingets nätverk.
- Åtkomst över nätverk är spårbar på så sätt att trafiken kan analyseras.
- Händelser i it-system följs upp kontinuerligt och onormala beteenden och avvikelser analyseras.
- Ramverk/principer/processer för ändringshantering, incidenthantering och problemhantering är etablerade.
- Tjänsternas säkerhetsnivå är verksamhetsmässigt avvägda gentemot informationens skyddsbehov/informationssäkerhetsklass.
- Tekniska lösningar för identitets- och autentiseringshantering motsvarar informationens skyddsbehov/informationssäkerhetsklass.
- Nätdesign styrs av principen separering av nättrafik i informationsproduktion och informationskonsumtion så att information i system och utrustning kan skyddas på rätt sätt.

Resultatmål

Indikator	Del-mål 2017	Mål 2020
Andel förvaltningar och bolag med it-drift som påbörjat arbete med att genomföra översyn av skyddet mot skadlig kod.	50 %	90 %
Andel förvaltningar och bolag med it-drift med ansvar för it-arbetsplats[8] som har påbörjat arbete med att införa it-säkerhet i standardiseringsarbetet.	50 %	90 %
Andel förvaltningar och bolag med it-drift som påbörjat arbete med att ta fram it-säkerhetsprinciper och rutiner för hantering av externa verksamheters utrustning som ansluts till egna nätverk.	50 %	90 %
Andel förvaltningar och bolag med it-drift som påbörjat arbete med att införa processer för ändringshantering, incidenthantering och problemhantering (där riskbedömningar av it-säkerheten ingår).	50 %	90 %
Andel förvaltningar och bolag med it-verksamhet[9] som genomför egenkontroller[10] av it- och informationssäkerhet.	50 %	90 %
Andel förvaltningar och bolag med it-verksamhet som påbörjat ett systematiskt arbete med att dokumentera kommunikationsbehov[11] via nätverk.	50 %	90 %
Andel förvaltningar och bolag med it-drift som påbörjat arbete med att ta fram principer för nätdesign med separering av nättrafik i produktion och konsumtion.	50 %	90 %
Andel av planerade aktiviteter som landstingets funktion för upptäckt och hantering av it-säkerhetsrelaterade hot och incidenter, SLL SOC, har avslutat gällande analys av onormala beteenden och avvikelser i it-system (dvs. anomalier).	50 %	90 %

[8] Med it-arbetsplats menas pc-arbetsplats, mobila utrustningar etc.
[9] Med it-verksamhet menas verksamhet med systemägarskap eller drift, dvs. ansvar för it-system.
[10] Med egenkontroll av informationssäkerhet menas kontroll i tre steg, dvs. deklaration, riskbedömning samt rapportering enligt landstingets s.k. compliance-process i nivå 3. Uppfyllandegrad ska anges.
[11] Med kommunikationsbehov avses både befintligt och framtida.

8. Styrmedel - så når landstinget målen

Ett framgångsrikt informationssäkerhetsarbete bygger på att alla, utifrån sina förutsättningar, tar ett ansvar för att vidta de åtgärder som behövs för att målen med informationssäkerhet ska nås. Vi behöver alla hjälpas åt i det arbetet.

För att dessa mål ska nås kommer det att krävas förändringar i våra beslutsmönster. Stockholms läns landsting ska arbeta med följande styrmedel för att driva på utvecklingen och nå målen inom rimlig tid: ledningssystem för informationssäkerhet, utbildning och kommunikation, riskbedömningar, säkerhetskrav i upphandling samt uppföljning. Detta är krav som redan ställs på landstingets verksamhet, men de måste vara uppfyllda för att handlingsprogrammet ska kunna genomföras.

Arbeta utifrån ledningssystem för informationssäkerhet

Landstinget har ett övergripande ledningssystem för informationssäkerhet som baseras på standarden SS-ISO/IEC 27000-serien. Landstingets nämnder, styrelser och bolag ska, inom ramen för det övergripande ledningssystemet för informationssäkerhet, tillämpa ett lokalt ledningssystem för informationssäkerhet.

En verkningsfull informationssäkerhet är en förutsättning för verksamheten och ger beslutsfattare och andra intressenter möjlighet att kunna förlita sig på att landstingets information är säker och skyddad. Genom att införa informationssäkerhet i relevanta verksamhetsprocesser åstadkoms en tydlig styrning mot uppsatta mål, ökad kontroll av att fastställda krav uppfylls samt en god informationssäkerhet.

Aktiviteter och åtgärder som krävs för att uppnå informationssäkerhetsmålen ska ingå i verksamhetsplanering, beslutsunderlag och budgetarbete. Respektive bolag och förvaltning ansvarar för att säkerställa att tillräckliga resurser avsätts för informationssäkerhetsarbetet samt att informationssäkerhetsmål och åtgärder förs in i verksamhetens handlingsplan och följs upp.

Kommunicera och utbilda kontinuerligt

För att lyckas med ett systematiskt informationssäkerhetsarbete och åstadkomma ett ökat säkerhetsmedvetande inom landstinget krävs dialog, både internt inom landstinget och externt. Planerade kommunikationsinsatser är därför nödvändiga för att hålla såväl medarbetare som externa aktörer informerade om vad som händer inom informationssäkerhetsområdet, men även för att ta emot förbättringsförslag. Under programperioden ska landstinget förbättra sin interna och externa kommunikation kring informationssäkerhetsarbetet.

För att lyckas krävs kunskap, engagemang och intresse. Därför ska all personal, inklusive respektive verksamhets ledning, genomgå grundläggande informationssäkerhetsutbildning, och ett block om informationssäkerhet ska ingå i landstingets chefsprogram.

Riskbedömning vid beslut
Landstingets verksamheter ska genomföra och dokumentera bedömningar av vilka hot, risker och sårbarheter som kan påverka verksamhetens information, och utifrån dessa vidta lämpliga skyddsåtgärder. Inför alla större beslut ska riskbedömningar gällande informationssäkerhet vara en del av beslutsunderlaget.

Ställa säkerhetskrav i upphandling
Varje år upphandlar landstinget it-system, produkter och tjänster för stora belopp i syfte att stödja informationshanteringen. Landstinget ska ställa krav vid upphandlingar så att upphandlade system och tjänster uppfyller landstingets informationssäkerhetskrav. Detta gäller även vid upphandling av molntjänster och vid outsourcing. Landstinget ska även kräva att våra leverantörer ska arbeta systematiskt med informationssäkerhet.

Följa upp och förbättra
Varje verksamhet inom landstinget ansvarar för att undvika överträdelser av författningsenliga eller avtalsmässiga skyldigheter relaterade till informationssäkerhet.

Landstingets informationssäkerhetskrav ska efterlevas och följas upp på alla relevanta nivåer. Det innebär bland annat att egenkontroller ska genomföras regelbundet i syfte att åstadkomma ständiga förbättringar. Förvaltningar och bolag ska minst årligen kontrollera sitt lokala ledningssystems lämplighet, tillräcklighet och verkan genom ledningens genomgång och då även följa upp sin handlingsplan.

9. Nationella strategier och handlingsplaner för informationssäkerhet

Myndigheten för samhällsskydd och beredskap, MSB, har i samarbete med Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, på regeringens uppdrag tagit fram en strategi för samhällets informationssäkerhet. Strategin gäller för perioden 2010-2015 och riktar sig till hela samhället. Strategin kompletteras med en nationell handlingsplan med konkreta åtgärder.

MSB har vidare tillsammans med Datainspektionen och Socialstyrelsen tagit fram en strategi för informationssäkerhet inom vård och omsorg specifikt. Strategin presenterades år 2012.

MSB anger i "Handlingsplan för skydd av samhällsviktig verksamhet" att samtliga aktörer som äger eller bedriver samhällsviktig verksamhet - det vill säga kommuner, landsting, länsstyrelser, centrala myndigheter och privata aktörer - ska ha integrerat ett systematiskt säkerhetsarbete i sin verksamhet på senast år 2020.

Regeringen har beslutat om "It i människans tjänst - en digital agenda för Sverige" och föreslagit ett nytt mål för it-politiken, Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Stockholms läns landsting har undertecknat en avsiktsförklaring om att i samverkan med olika samhällsaktörer stödja framtagandet av en regional digital agenda. Den syftar till att skapa ett digitalt "innanförskap", där it är enkelt och säkert att använda, där e-tjänster skapar nytta och där den grundläggande infrastrukturen skapar förutsättningar för informationen att behandlas på ett säkert sätt.

Med Stockholms läns landstings handlingsprogram för informations-säkerhet bidrar vi till ambitionerna i de nationella handlingsplanerna.

10. Referenser

Näringsdepartementet: It i människans tjänst - en digital agenda för Sverige. N2012/6402/ITP. Oktober 2011.

Myndigheten för samhällsskydd och beredskap, MSB: Strategi för samhällets informationssäkerhet 2010-2015. November 2011.

Myndigheten för samhällsskydd och beredskap, MSB: Samhällets informationssäkerhet. Nationell handlingsplan 2012. Augusti 2012.

Myndigheten för samhällsskydd och beredskap, MSB: Strategi för stärkt informationssäkerhet inom vård och omsorg. Maj 2014.

Myndigheten för samhällsskydd och beredskap, MSB: Handlingsplan för skydd av samhällsviktig verksamhet. December 2013.

Stockholms läns landsting: Avsiktsförklaring om regional digital agenda. LS 1301-0117. Mars 2015.

Stockholms läns landsting: Mål och budget 2016 inklusive beslutssammanfattning. LS 2015-0039, LS 1312-1542. Oktober 2015.

Stockholms läns landsting: Informationssäkerhetspolicy för Stockholms läns landsting. LS 1112-1733. Mars 2013.

Stockholms läns landsting: Riktlinjer för Stockholms läns landsting. LS 1112-1733. Mars 2013.

Stockholms läns landsting: Krisberedskapsplan för Stockholms läns landsting och plan för krisledningsnämnden vid extraordinära händelser. LS 1406-0750. Mars 2015.

Centrala samverkansgruppen

UTDRAG FRÅN
MINNESANTECKNINGAR
2016-02-10

LS 1308-1044

Utdrag ur minnesanteckningarna förda vid möte med centrala samverkansgruppen den 10 februari 2016

Punkt 3

Slutbehandling av handlingsprogram för informationssäkerhet

Centrala samverkansgruppen har tagit del av landstingsdirektörens tjänsteutlåtande handlingsprogram för informationssäkerhet LS 1308-1044 med bilagor.

Muntlig information i ärenden lämnades på Centrala samverkansgruppens möte den 13 januari av informationssäkerhetschef, Vesna Lucassi

landstingsdirektörens tjänsteutlåtande handlingsprogram för informationssäkerhet LS 1308-1044 med bilagor var utsänt förmötet den 13 januari.

På dagens möte svarade informationssäkerhetschef, Vesna Lucassi på frågor om ärendet.

Arbetsgivaren konstaterar att ärendet härmed är slutbehandlat.

Vid protokollet
Lena Halvardson Rensfelt

Exp.
Akten
Landstingsstyrelsen