NÄSSJÖ KOMMUN

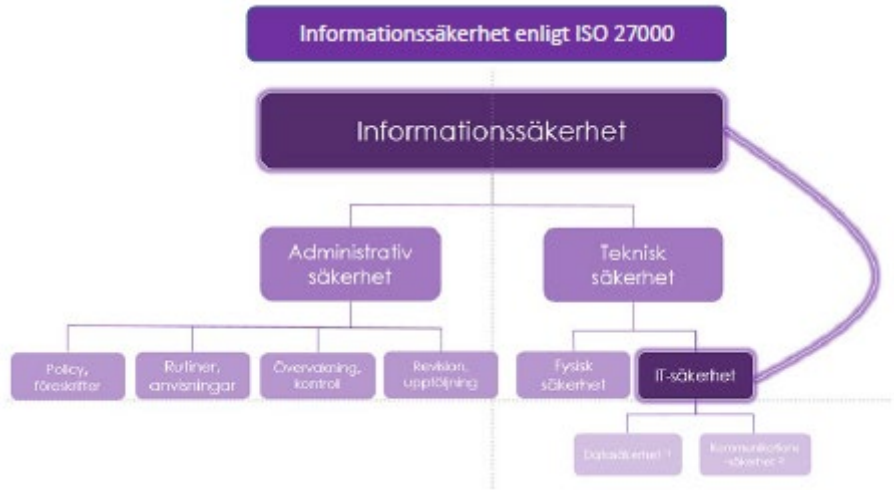
Författningssamling

Dokumenttyp Policy	Beslutsinstans Kommunfullmäktige	Beslutsdatum 200326	§ 60
Dokumentansvarig Höglandets IT Kommunledningskontorets E-strateg			
Gäller för Nässjö kommun (Höglandsgemensam)		**Senast reviderad** -	

IT-säkerhetspolicy

Om IT-säkerhetspolicyn

IT-säkerhetspolicyn är ett dokument som redovisar Höglandsförbundets och dess medlemskommuners övergripande mål och inriktning med IT-säkerheten samt hur ansvaret i dessa frågor är fördelat.
Denna policy gäller för IT-säkerhet inom höglandssamarbetet, och kompletterar förbundets och kommunernas övriga styrdokument inom säkerhetsområdet. Hela kommunkoncernen omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna. IT-säkerhetsarbetet ska vara systematiskt och bygga på etablerade standarder inom ISO 27000-serien.



Enligt förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (SFS 2015:1052 med ändring i SFS 2018:668) framgår att varje

myndighet, eller annan offentlig verksamhet, ansvarar för att egna system uppfyller sådana grundläggande och särskilda säkerhetskrav så att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och dess tillhörande förordning (2018:1175) ställer särskilda krav på leverantör av samhällsviktiga och digitala tjänster. Syftet är att uppnå en tillräckligt hög nivå på säkerheten i nätverk och i informationssystem för samhällsviktiga tjänster, grunden är det så kallade NIS-direktivet.

Om IT-säkerhet

IT-säkerhet handlar om att skydda verksamhetens IT-relaterade tillgångar, som maskinvara, programvara och den information som lagras och hanteras i dessa. IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av digital teknik. Informationens skyddsvärde avgör vilka krav som ställs vad gäller tekniska skyddsåtgärder.
IT-säkerhetsarbete innebär att kontinuerligt och långsiktigt arbeta med att utforma, införa, övervaka, granska och vid behov förbättra rutiner, processer, organisation och tekniska skydd som behövs för att säkerställa att verksamhetens mål och skyddsbehov för informationen uppnås.

Mål med IT-säkerhet

Målsättning med IT-säkerhetsarbetet är att säkerställa en robust och säker drift. Det innebär en hög tillgänglighet till kommunikationsnät och digitala resurser så att de kan nyttjas till dess avsedda funktion. Särskilt viktigt är att förhindra att störningar orsakar allvarliga konsekvenser för kommunen eller dess invånare.

Information som behandlas, det vill säga skapas, förändras, överförs, lagras eller raderas, ska skyddas mot oavsiktlig eller obehörig förändring, förstöring, åtkomst eller kopiering.

IT-säkerhetsarbetet ska verka för att säkerställa skyddet mot avsiktliga intrång, otillåten användning, stöld och skadegörelse och även omedvetna handlingar som brister i arbetsprocessernas säkerhet samt mänskliga misstag. Åtgärder för att uppnå målen för IT-säkerheten väljs i förhållande till kostnader, säkerhetsnivåer, risker, konsekvenser vid störningar och deras inverkan på den dagliga verksamheten.

Principer och arbetssätt

Höglandsförbundet och dess medlemskommuner ska arbeta med IT-säkerhet på ett sätt så att ovanstående mål uppfylls.

Arbetet med IT-säkerhet inom Höglandsförbundet och dess medlemskommuner ska:

- följa antagen Informationssäkerhetspolicy och dess principer och arbetssätt. Genom Ledningssystemet (LIS) arbetas det kontinuerligt med att utforma, införa, övervaka, granska och vid behov förbättra skyddsåtgärder. Utöver detta ska lag- och myndighetskrav beaktas.

- regelbundet genomföra risk- och sårbarhetsanalyser för IT-säkerhetens relevanta delar. Åtgärder för att möta identifierade hot och risker ska dokumenteras i systemets förvaltningsplan.

- bedrivas förebyggande, långsiktigt och kostnadseffektivt samt utgå från lagar, förordningar, föreskrifter, verksamhetskrav och avtal. Arbetet ska genomföras

på ett välstrukturerat sätt i samverkan mellan kommunerna och Höglandsförbundet.

- vid upphandling och utveckling av IT-tjänster och system, ta hänsyn till krav utifrån informations- och IT-säkerhet. Det regleras i kravspecifikation och avtal, om det inte är uppenbart onödigt.

- säkerställa att systemens skyddsbehov baseras på informationsklassning och dokumenteras i systemets förvaltningsplan. Kraven regleras i upprättat avtal med driftsleverantör. Åtgärder för att säkerställa IT-drift dokumenteras i systemdokumentation hos driftsleverantör.

- säkerställa att samtliga personer som på något sätt använder digitala resurser ska ha den information och utbildning som är nödvändig för att de ska kunna upprätthålla den IT-säkerhetsnivå som krävs av dem.

- säkerställa att samtliga system är identifierade och förtecknade och att systemägare och systemansvarig är utsedda.

Höglandsförbundet ska:

- systematiskt spåra användaraktiviteter, exempelvis avvikelser, fel och informations-säkerhetshändelser. Underlag skapas via loggning, granskning av underlag ska ske regelbundet av Höglandets IT.

Roller och ansvar

Grundprincipen är att ansvaret för IT-säkerheten följer verksamhetsansvaret inom Höglandsförbundet och dess medlemskommuner. För enskilda system har systemägaren ansvaret för IT-säkerheten. Arbetet med att upprätta en tillräckligt god IT-säkerhet ska samordnas mellan Höglandsförbundet och dess medlemskommuner. Höglandsförbundet ansvarar för medlemskommunernas tekniska infrastruktur. Organisation, ansvarsfördelning och roller ska säkerställa att ett system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid stödjer verksamheten på avsett sätt och bidrar till att uppfylla verksamhetens mål.

Nedan beskrivs IT-säkerhetsansvaret för ett antal roller. Ansvar och tillhörande uppgifter för respektive roll beskrivs utförligare i riktlinjer inom informationssäkerhetsområdet.

Höglandsförbundets direktion ansvarar för framtagande av IT-säkerhetspolicyn. Policyn tas fram i samverkan mellan Höglandsförbundet och dess medlemskommuner. Vid behov, eller minst en gång per mandatperiod, ska direktionen initiera aktualitetsprövning av policyn. Direktionen ansvarar för Höglandsförbundets övergripande IT-säkerhet.

Förbundsdirektören ska på uppdrag av direktionen se till så att IT säkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer. Förbundsdirektören ansvarar för att övergripande riktlinjer utarbetas och hålls aktuella i enlighet med policyn.

IT-chefen är systemägare för förbundets IT-tekniska infrastruktur och samverkar med övriga systemägare avseende systemens tekniska drift. I detta ingår bland annat att svara

för systemens tekniska säkerhet och säkerställa att nätverk, kommunikation, lagring och serverplattform har tillräcklig kapacitet i den tekniska infrastrukturen.

Kommunfullmäktige i respektive medlemskommun godkänner den höglands-gemensamma IT-säkerhetspolicyn.

Kommundirektör och Vd för respektive medlemskommun har det övergripande ansvaret för IT-säkerheten inom den egna kommunen alternativt bolaget. I uppdraget ingår att se till att IT-säkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer. Arbetet ska ske i samverkan med Höglandsförbundet.

Systemägaren ska säkerställa att systemet har en dokumenterad förvaltningsplan. I denna plan ska skyddsbehovet finnas fastställt. Skyddsbehovet anger krav på driftsmiljön och ska regleras i avtal. En risk- och sårbarhetsanalys ska genomföras regelbundet för att identifiera och fastställa nödvändiga skyddsåtgärder. Planering för genomförande av skyddsåtgärder och handlingsplan ska finnas dokumenterat i förvaltningsplanen. I händelse av incidenter som kan få en negativ påverkan på informationssäkerheten ska även dessa skyddsåtgärder dokumenteras i förvaltningsplanen. Förvaltningsplanen ska delges Höglandets IT eller annan driftsansvarig.

Systemansvarig säkerställer att varje användare har rätt behörighetsnivå och tillräckliga kunskaper för att använda systemet på ett säkert och ändamålsenligt sätt. Systemansvarig ska bistå systemägaren med framtagande och efterlevnad av förvaltningsplan.

Driftsansvarig ska säkerställa att den tekniska driftsmiljön uppfyller de krav som systemägaren beskriver i systemets förvaltningsplan. Uppfyllande av krav regleras i avtal. Beskrivning av driftsmiljö och rutiner för daglig systemdrift, inklusive ändringshantering, samt hantering av extra ordinära händelser ska noteras i systemdokumentationen.

IT-säkerhetsrådet på Höglandets IT ska driva det strategiska och operativa arbetet med IT-säkerhetsfrågor i samverkan med verksamheternas funktionella krav och behov.