GRUNDLÄGGANDE RIKTLINJE FÖR
INFORMATIONSSÄKERHET

ANEBY • EKSJÖ • NÄSSJÖ • SÄVSJÖ • VETLANDA

HÖGLANDS-
FÖRBUNDET

2023-09-15

Grundläggande riktlinje för informationssäkerhet

Om den här grundläggande riktlinjen för informationssäkerhet

Riktlinjen vänder sig till de kommuner och förbund som ingår i höglandssamarbetet inkluderat deras förvaltningar, ledningsgrupper och de som genom en tilldelad roll kommer att arbeta med informationssäkerhet.

Riktlinjen redogör för de roller som är identifierade och beskriver övergripande deras funktion och ansvar samt hur förutsättningar skapas så att kommunen eller förbundet kan planera och följa upp informationssäkerhetsarbetet.

Denna riktlinje för medlemskommunerna Aneby, Eksjö, Nässjö, Sävsjö och Vetlanda med förbund är beslutad av informationssäkerhetsnätverket 2023-08-22 och fastställd av kommundirektörerna 2023-09-15.

Innehåll

1 Inledning

Information är en av våra viktigaste tillgångar. För att skydda informationen behövs ett säkerhetsmedvetande hos alla anställda och förtroendevalda. Det innebär att information finns tillgänglig när den behövs, är korrekt och att obehöriga inte får åtkomst till den. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån de tre egenskaperna: tillgänglighet, riktighet och konfidentialitet. I praktiken innebär det att vi ska ha tillgång till den information vi behöver vid rätt tillfälle, att vi kan lita på informationen och att inte obehöriga kan ta del av den.

För att minska konsekvenserna vid incidenter är ett systematiskt och riskbaserat informationssäkerhetsarbete väsentligt. Ett fungerande informationssäkerhetsarbete syftar till att förebygga och hantera allvarliga störningar och kriser. Därmed säkerställs skyddet för information och förtroendet för verksamheternas informationshantering både i och utanför IT-system.

Ett systematiskt informationssäkerhetsarbete kommer kommuninvånarna till nytta genom att deras rättigheter och personliga integritet skyddas.

Denna riktlinje utgår från informationssäkerhetspolicyn och ska brytas ner till verksamhetsspecifika handlingsplaner.

2 Skapa förutsättningar för informationssäkerhetsarbetet inom den egna kommunen eller förbundet

2.1 Handlingsplan och uppföljning

En fastställd årlig handlingsplan är ett stöd för kommunen eller förbundet i informationssäkerhetsarbetet genom att dokumentera aktiviteter, sätta tidsplan samt utse ansvariga för olika aktiviteter. Arbetet ska genomföras på ett sådant sätt att lokal informationssäkerhetssamordnare med stöd av informationssäkerhetsspecialist på ett enkelt sätt kan följa upp informationssäkerhetsarbetet och hur dess planering är tänkt samt att detta avrapporteras till kommunens eller förbundets ledning.

2.2 Tillräckliga resurser

Informationssäkerhet är ett komplext område som berör hela organisationen. För att kommunen eller förbundet ska kunna efterleva krav och förväntningar på informationssäkerhet behöver roller avseende informationssäkerhet utses. Personer som tilldelas dessa roller behöver dessutom ges förutsättning för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive kommun/förbund.

2.3 Informationskartläggning

Alla organisationers verksamhet bygger idag på komplexa strukturer av informationshantering. För att kunna skapa ett fungerande informationssäkerhetsarbete måste informationen vara identifierad och beskriven. För att kunna arbeta systematiskt måste kommunen/förbundet därför kartlägga den information som hanteras i informationshanteringsplaner.

2.4 Informationsklassning

Ett av de mest grundläggande och viktigaste verktygen i informationssäkerhetsarbetet är informationsklassningen. Informationsklassningen syftar till att göra en bedömning av hur kritisk information är för verksamheten och vilka skyddskrav som finns från författningar för att säkerställa skyddsnivå gällande konfidentialitet, riktighet och tillgänglighet.

2.5 Systemförvaltning

Kommunerna och förbunden behöver säkerställa att egna system är identifierade och informationsklassade för att säkerställa rätt skyddsnivå. Aktiviteter för att uppnå rätt skyddsnivå ska finnas dokumenterade i förvaltningsplaner, vilka följs upp av systemägarna.

3 Roller och ansvar

3.1 Kommundirektör och förbundsdirektör

Kommundirektörens och förbundsdirektörens uppdrag är att säkerställa att organisationens hela informationssäkerhetsarbete bedrivs så effektivt som möjligt utifrån gällande policydokument, metodhandbok och riktlinjer.

Säkerhetsskydd som även omfattar informationssäkerhet för de säkerhetsskyddsklassificerade uppgifterna regleras inom respektive organisations säkerhetsskyddsarbete och leds av säkerhetsskyddschef.

3.2 Förvaltningschef eller motsvarande

Förvaltningschef eller motsvarande är informationsägare och har ett övergripande ansvar för informationssäkerhet inom sin verksamhet. Förvaltningschefen ska säkerställa att förvaltningens informationssäkerhetsarbete bedrivs enligt denna grundläggande riktlinje samt avsätta tillräckliga resurser i form av tid och säkerställt mandat inom egen förvaltning för att nå en tillräcklig nivå av informationssäkerhet.

Ansvarar också, i egenskap av informationsägare, för att nämndernas dokumenthanteringsplaner/informationshanteringsplaner upprättas och hålls uppdaterade. Arkivarie eller motsvarande resurs inom kommunen har en stödjande funktion i denna process. Dokumenthanteringsplaner/informationshanteringsplaner samlar alla informationstillgångar som finns i en verksamhet, och planerna kan vara till hjälp i informationssäkerhetsarbetet och vid informationsklassningar.

Förvaltningschefen ska även rapportera status på informationssäkerhetsarbetet till berörda nämnder, kommundirektören och till lokal informationssäkerhetssamordnare.

3.3 Verksamhetschef och enhetschefs nivå

Verksamhetschef/enhetschef ansvarar för informationssäkerheten inom sitt ansvarsområde. Verksamhetschef/enhetschef ansvarar för att egna medarbetare kontinuerligt uppdateras och med bibehållet säkerhetsmedvetande har tillräcklig förståelse och kunskap för att en tillräcklig informationssäkerhet i verksamheten kan uppnås.

3.4 Lokal informationssäkerhetssamordnare

Varje kommun och förbund ska utse representant för lokal samordning inom området informationssäkerhet. Informationssäkerhetssamordnaren ska ges förutsättning för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive kommun/förbund.

Den lokala informationssäkerhetssamordnaren representerar egen kommun eller förbund i Höglandets informationssäkerhetsnätverk.

Den lokala informationssäkerhetssamordnaren ska samordna och bjuda in till lokala möten med förvaltningarnas informationssäkerhetsresurser. Planering av mötesinnehåll kan göras med stöd av informationssäkerhetsspecialist.

Den lokala informationssäkerhetssamordnaren ska med stöd av informationssäkerhetsspecialist ta fram förslag på årlig handlingsplan för den egna kommunens eller förbundets informationssäkerhetsarbete. Årlig handlingsplan ska fastställas av kommunledning eller förbundsledning.

Lokal informationssäkerhetssamordnare bör delta i regionala och nationella informations-säkerhetsmöten.

Varje lokal informationssäkerhetssamordnare behöver få nödvändig kompetens inom informationssäkerhetsområdet, vilken kan erhållas genom en samordnadgrundutbildning i kombination med kompletteringsutbildningar vid behov.

3.5 Informationssäkerhetsresurs på förvaltning

Varje förvaltning behöver utse en eller flera informationssäkerhetsresurser för att stödja förvaltningen (ledningsgrupp och medarbetare) i sitt informationssäkerhetsarbete. Resursen ska delta i lokalt nätverk för informationssäkerhet.

Det är viktigt att denna informationssäkerhetsresurs är en person som har god kännedom om förvaltningen och dess olika processer och verksamheter.

Varje informationssäkerhetsresurs behöver få nödvändig kompetens inom informations-säkerhetsområdet genom höglandsgemensam internutbildning.
Informationssäkerhetsresursen ska kunna tillämpa metodstöd.
Informationssäkerhetsresursen ska ha förutsättning för att kunna utföra uppdraget. Tid, kompetens och mandat bedöms utifrån vilka områden som ska prioriteras inom respektive förvaltning.

3.6 Medarbetare

Varje medarbetare har ett eget ansvar för att vara uppmärksam på brister och fel gällande informationshantering, utrustning och informationsinnehåll samt att rapportera brister och fel enligt fastställda rutiner.

3.7 Systemägare

Systemägaren är informationsansvarig för systemets information. En viktig del i ansvaret är att besluta om tillgångens skyddsnivå genom informationsklassning och kontinuerliga riskanalyser. Ansvaret sträcker sig till att systemägaren ska säkerställa att det för uppgifterna som hanteras i, importeras till eller exporteras från systemet finns etablerade rutiner i form av användarinstruktioner och att utbildning ges till den som ska arbeta i systemet.

Systemägaren ska säkerställa att det för systemet finns en förvaltningsplan som hålls aktuell och följs. Systemägaren ska utse systemansvarig samt säkerställa att personuppgiftsbiträdesavtal finns för systemet.

3.8 Systemansvarig (systemförvaltning, super-user, systemadministratör)

Systemansvarig är den eller de personer som har ansvaret för den dagliga användningen av systemet. Systemansvarig förväntas vara kunnig på systemets funktionalitet, ständigt jobba med förbättring och utveckling samt att underhålla behörighetsroller.

3.9 Höglandets informationssäkerhetsnätverk

Höglandets nätverk för informationssäkerhet bedriver det övergripande och strategiska arbetet med att utveckla och samordna informationssäkerhetsarbetet för medlems-kommunerna och förbunden.

I nätverket arbetar Höglandsförbundets informationssäkerhetsspecialister i samråd med kommunernas och förbundens lokala informationssäkerhetssamordnare vad gäller informationssäkerhet.

Nätverket genomför regelbundna möten.

3.10 Höglandsgemensamma informationssäkerhetsspecialister

Vid Höglandsförbundet finns gemensamma informationssäkerhetsspecialister som stöttar de kommuner och förbund som ingår i höglandssamverkan.

Informationssäkerhetsspecialisterna ger stöd och råd i tolkning av informations-säkerhetskrav och metodstöd.

Informationsspecialisterna samordnar den höglandsgemensamma utvecklingen av informationssäkerhetsarbetet och är sammankallande för Höglandets informationssäkerhetsnätverk med representanter från samtliga kommuner och förbund.

Informationsspecialisterna är rådgivande expertstöd avseende informationssäkerhet vid projekt och upphandlingar.

Informationsspecialisterna identifierar utbildningsbehov i samverkan med informationssäkerhetsnätverket, tar fram utbildningsmaterial och genomför utbildningar.

Informationssäkerhetsspecialisterna genomför även omvärldsbevakning inom informationssäkerhetsområdet, bland annat genom deltagande i regionala och nationella samarbeten och informationssäkerhetsnätverk. Informationsspecialisterna delger informationen från denna bevakning till informationssäkerhetsnätverkets medlemmar.

3.11 Dataskyddsombud

För att uppfylla de krav som dataskyddsförordningen ställer finns ett gemensamt dataskyddsombud för de kommuner och förbund som ingår i höglandssamverkan. Dataskyddsombudet har en rådgivande roll och en oberoende ställning. Dataskyddsombudet utövar tillsyn för att säkerställa att personuppgifter behandlas på ett korrekt sätt i verksamheten.

3.12 Arkivarier eller motsvarande

Arkivarier, arkivassistenter eller motsvarande har en rådgivande roll vid framtagande av de dokumenthanteringsplaner/informationshanteringsplaner som finns i kommunens/förbundets verksamheter och som beslutas av nämnderna.

Arkivarier, arkivassistenter och motsvarande kan med fördel medverka i lokala och höglandsgemensamma informationssäkerhetsnätverk.

Arkivarien är en stödfunktion vid informationsklassningsarbete, både inför upphandling av nya IT-system och av verksamheters information i befintliga IT-system. Det är särskilt viktigt att ha med arkivfunktionen vid upphandling av nya IT-system för att säkerställa att hänsyn tas till arkivkrav.

3.13 IT-säkerhetsorganisation inom Höglandsförbundet

Höglandets IT ansvarar för att säkerheten i IT-miljön är tillförlitlig och motsvarar verksamheternas och legala krav. IT-miljön ska även uppfylla de krav informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet ställer. Höglandsförbundets antagna IT-säkerhetspolicy styr detta arbete.

Inom Höglandets IT finns enheten för IT-säkerhet och arkitektur som har i uppdrag att driva det strategiska och operativa arbetet med IT-säkerhetsfrågor i samverkan med verksamheternas funktionella krav och behov. Enheten innefattar enhetschef tillika IT-säkerhetsansvarig, IT-säkerhetsspecialister och IT-arkitekter. Tillsammans med detaljspecialister finns även ett IT-Säkerhetsråd som har i uppgift att hantera operativa IT-säkerhetsfrågor, etablera riktlinjer och rutiner, omvärldsbevaka och utbilda.