VÄRNAMO KOMMUN

Reglemente
Policy
Plan
Åtgärdsplan
Riktlinje

Riktlinje - Informationssäkerhet

Reglemente
Kommunala beslut som utöver kommunallag och andra författningar styr och reglerar kommunala verksamheter. Innefattar Nämndreglementen, Delegeringsordningar, Bolagsordningar, Ägardirektiv, Föreskrifter, Kommunala taxor och avgifter.

Policy
Anger principer och värdegrundsbaserat förhållningssätt och tjänar som vägledning inom det aktuella området.

Plan
Beskriver strategier för arbetet med utvecklingen av Värnamo som kommun, och utvecklingsarbete inom kommunens organisation.

Åtgärdsplan
Anger konkreta åtgärder, tidsramar och ansvar.

Riktlinje
Beskriver hur förvaltning bedriver den befintliga verksamheten, eller ett visst område, så att den bedrivs effektivt och med god kvalitet.

Fastställd av: Kommundirektören
Dokumentet gäller från: 2022-04-21
Dokumentet gäller för: Kommunövergripande
Dokumentansvarig: Kommundirektör**,** Kommunledningsförvaltningen

Bakgrund

Kommunens informationssäkerhet omfattar alla verksamheters informationstillgångar, både information som hanteras digitalt och analogt. Detta dokument, Riktlinje - informationssäkerhet, konkretiserar kommunens informationssäkerhetspolicy med information och regler för hur information får hanteras inom kommunen, och beskriver vad som behöver etableras för att uppfylla informationssäkerhetspolicyn och integrera informationssäkerhetsarbetet som en naturlig del i verksamheterna.

För att uppnå verksamhetsmål och för att invånare, myndigheter, samarbetspartner och anställda ska känna förtroende för kommunen, behöver arbetet med informationssäkerhet vara en naturlig integrerad del i kommunens kvalitetssystem, verksamhetsutveckling och förvaltning, och inarbetas i den egna verksamhetens lokala handlingsplaner och rutiner.

Syfte

Syftet med riktlinjen är att förtydliga roller i informationssäkerhetsarbetet, innehåll i ledningssystem för informationssäkerhet, samt att säkerställa att vi agerar korrekt och håller god kvalitet när vi hanterar information. Riktlinjen ska vara stöd i arbetet med att skapa och upprätthålla lämpligt skydd av information.

Organisation och ansvar

I Policy informationssäkerhet beskrivs nämnders och förvaltningars ansvar för att organisera arbetet så att de informationssäkerhetskrav som ställs på verksamheten efterlevs. Det innebär att varje förvaltning behöver fastställa organisation med utpekade roller.

Roller

Verksamhetsansvar: Ansvaret för informationssäkerhet följer verksamhetsansvaret med särskilt ansvar på chefsnivå. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. I detta ingår även ansvar för att medarbetare utbildas, att verksamhetsnära riktlinjer, rutiner och instruktioner tas fram, samt kontinuitetsplaner för att hantera avbrott. Varje **medarbetare** ansvarar för att följa styrdokument och rutiner samt att upptäckta brister rapporteras.

Den verkställande rollen som **informationsägare** har ansvaret för att informationen i system och processer inom verksamhetsområdet hanteras och förvaltas på ett säkert sätt. Informationsägaren är också **riskägare** för den information som hanteras, digitalt eller på annat sätt, och därmed ansvarig för att informationsklassning och riskanalyser genomförs, och att krav och behov beskrivs. Om informationsägare inte är utsedd innehas den verkställande rollen av förvaltningschef.

Den verkställande rollen som **systemägare** har mandat och medel för att fatta de avgörande besluten om informationssystemets vidareutveckling och avveckling, och ansvarar för att handlingsplan tas fram och hanteras i samband med övrigt kommunövergripande budgetarbete. Om systemägare inte är utsedd innehas den verkställande rollen av förvaltningschef.

Systemansvarig/systemförvaltare bereder systemärenden, svarar för administration, förvaltning och användning av informationssystem.

Projektägare/beställare säkerställer att informationssäkerheten beaktas och ansvarar för att fastställa informationssäkerhetsnivå i projektet och projektets resultat. **Projektledare** ansvarar tillsammans med **styrgrupp** för informationssäkerheten beaktas och efterlevs under hela projekttiden.

IT-centerchef innehar det verkställande ansvaret för att kommunens IT-driftmiljö och infrastruktur bedöms motsvara verksamheters krav på IT-säkerhet, och att i samverkan med informationsägare och systemägare uppnå adekvat nivå på säkerhetsåtgärder för system och information.

Kommunens **säkerhetsgrupp** har en samordnande funktion i arbetet med kommunens interna säkerhetsarbete och tar fram underlag, analyser och förslag på beslut till kommunens förvaltningsledningsgrupp. Arbetsgruppen ska samordna de uppgifter och uppdrag som beslutas av kommunens ledningsgrupp och erbjuda stöd till de funktioner som arbetar med uppdragen på förvaltningsnivå.

Informationssäkerhetssamordnare leder och samordnar kommunens informationssäkerhetsarbete, ansvarar för att ta fram förslag till övergripande policy, riktlinjer och rutiner, utveckling av metoder, samt stödjer verksamheterna i frågor som rör informationssäkerhet. Informationssäkerhetssamordnaren följer upp informationssäkerhetsarbetet, samt rapporterar till kommundirektör och dennes ledningsgrupp.

Ledningssystem för informationssäkerhet

Utifrån Policy - informationssäkerhet, och Riktlinje - informationssäkerhet, kan övergripande ämnesspecifika eller verksamhetsspecifika riktlinjer, instruktioner, processbeskrivningar, rutiner och metodstöd behöva upprättas.

För att realisera ett ledningssystem för informationssäkerhet behöver arbetet med informationssäkerhet omfatta: informationsklassning, risk- och sårbarhetsanalys, incidenthantering, kontinuitetsplaner för att hantera avbrott – tillfälliga eller i kris, samt uppföljning av åtgärder och återkoppling. Arbetet ska vara en naturligt integrerad del i Värnamo kommuns ledningssystem, verksamhetsutveckling och förvaltning och kontinuerligt utvärderas och anpassas till gällande omvärlds- och verksamhetskrav.

Sammantaget utgör detta Värnamo kommuns Ledningssystem för informationssäkerhet.

Informationssäkerhet i verksamhetsnära förvaltning

Personalsäkerhet

Bakgrundskontroll på den som söker anställning bör utföras i förhållande till vilken information personen ska ges tillgång till och vilka risker som kan uppstå.

Medarbetare ska ges tillräcklig information om sin roll och ansvar för informationssäkerhet innan de ges åtkomst till känslig information eller informationssystem. Detta innefattar information om det egna ansvaret för att följa regelverk, att skydda autentiseringsinformation och information, att endast ta del av information som behövs för att kunna utföra sina arbetsuppgifter, att logguppföljning utförs, samt vilka påföljder som kan bli aktuella om regelverk inte efterlevs.

Informationstillgångar och informationsklassning

Alla informationstillgångar ska förtecknas i dokumenthanteringsplan och ha en utsedd informationsägare. Med informationstillgångar avses till exempel informationssystem och/eller processer och dess information, eller pappers- eller digitala handlingar.

Informationstillgångarna ska klassificeras. Detta innebär att man på ett enhetligt sätt värderar organisationens information med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet, utifrån vilka konsekvenser ett otillräckligt skydd skulle kunna få. Som stöd för informationsklassning används kommunens rutin samt SKR:s systemstöd KLASSA.

Skydd av personlig integritet och personuppgifter ska säkerställas i enlighet med gällande författningar.

Känslig eller sekretessbelagd information hanteras i första hand inom därför avsedda system.

Riskanalys

Riskanalys ska genomföras regelbundet och vid större förändringar, exempelvis större systemuppdateringar, nyanskaffning, nya användargrupper eller extern åtkomst. Även förändringar utanför system eller dess kontroll motiverar en riskanalys, exempelvis ägarbyte av systemleverantör, förändrade rättsliga krav, omorganisation eller väsentliga förändringar av arbetsrutiner för viktiga eller kritiska informationstillgångar. Beslut om åtgärdsgrad samt tidsram fattas av informationsägare som tillika är riskägare. Riskanalysens resultat ska dokumenteras och följas upp. Som stöd för riskanalys används kommunens rutin samt SKR:s systemstöd KLASSA.

Incidenthantering

Informationssäkerhetsincidenter ska inrapporteras via fastställda rapporteringsvägar. Alla anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster ska notera och rapportera observerade eller misstänkta säkerhetsbrister i system eller tjänster.

Processer och rutiner ska finnas för att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation i samband med incidenterna.

Kontinuitetshantering

Informationsägaren ska fastställa hur länge avbrott i åtkomst till verksamhetssystem är acceptabla, det vill säga: hur länge man vid avbrott kan bedriva verksamhet utan stora svårigheter.

Juridiska krav samt verksamhetens behov av tillgång till information ska dokumenteras och riskbedömning genomföras. I sammanhanget ska även nyckelpersonberoende analyseras. Kontinuitetsplaner ska upprättas för att

säkerställa fortlöpande verksamhet. Detta innefattar reservrutiner och övriga åtgärder som kan vidtas vid IT-avbrott, exempelvis manuella rutiner. Om verksamheten är beroende av en annan organisation, exempelvis en annan förvaltning, avdelning eller en leverantör, ska även dessa involveras i arbetet.

Fysisk och miljörelaterad säkerhet

Den fysiska säkerheten skall organiseras så att verksamhetens medarbetare och uppdragstagare, lokaler, utrustning och informationstillgångar skyddas mot hot som inbrott, stöld, brand, översvämning, olyckor och katastrofer som orsakas av fel i tekniska system, misstag, sabotage eller andra händelser.

Styrning av åtkomst och loggning

Åtkomst till information och system inom kommunen ska styras med hjälp av organisatoriska och tekniska skyddsåtgärder såsom behörighetsstyrning, åtkomstkontroll, loggning och logguppföljning. Åtkomsten ska bygga på verksamhetens säkerhetskrav och behov, och vara baserad på roller, ansvars- och arbetsområde.

Användare ska ha individuella användaridentiteter. Det ska finnas formella processer för registrering och avregistrering av användare, tilldelning av åtkomsträttigheter till system och tjänster och tilldelning av autentiseringsinformation.

Vid åtkomst till information med höga skyddskrav på konfidentialitet och/eller riktighet ska stark autentisering användas, eller plan tas fram för införande. Stark autentisering är krav vid fjärråtkomst till Värnamo kommuns IT-miljö.

Priviligierade åtkomsträttigheter ska begränsas och styras till att omfatta de uppdrag som användaren har utbildning, ansvar och befogenheter att utföra. Priviligierade åtkomsträttigheter ska ha en användaridentitet skild från den som används i den ordinarie verksamheten.

För externa användare (konsult/entreprenör) gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning, även ska vara tidsbegränsad för den tid som behövs för att utföra uppgiften. Tilldelningen ska föregås av sekretessavtal.

Loggar ska produceras i den utsträckning som krävs för att verksamheten ska kunna förebygga, upptäcka och rätta till relevanta fel och felaktigheter, oönskade händelser och förändringar i information, samt följa upp att gällande regelverk efterlevs.

Informationsägare ansvarar för att regelbunden granskning av användarnas olika åtkomsträttigheter genomförs, samt för att loggar i verksamhetsspecifika system regelbundet granskas.

Leverantörsrelationer.

Informationssäkerhet ska inkluderas i kraven för nya informationssystem eller förbättringar av befintlig informationshantering. En riskanalys ska alltid föregå nyanskaffning och större förändringar oavsett om informationssystemet eller tillämpningen levereras internt eller externt som någon form av molntjänst.

Informationssäkerhet i IT-miljön

Hantering av tillgångar

Det ska finnas aktuella förteckningar över IT-inventarier och programvarulicenser.

Det ska finnas aktuell dokumentation över hård- och mjukvara som används i enskilda informationssystem, beroenden mellan olika interna informationssystem, respektive beroenden av informationssystem hos externa aktörer, vilka informationssystem som behandlar information som har behov av utökat skydd, och vilka informationssystem som är centrala för kommunens förmåga att utföra sitt uppdrag. Aktuell beskrivning av IT-miljö, teknisk plattform och återstartsplaner ska upprätthållas.

Rutiner för återlämning och destruering av datorer och handhållen utrustning ska finnas och göras kända för verksamheterna.

Säkerhetskopiering

Säkerhetskopior av information och programvara ska tas och testas regelbundet. Rutinerna för säkerhetskopiering och återläsning ska vara väl utvecklade, så att informationens och IT-miljöns riktighet, tillgänglighet och avsedda funktion skyddas. Likaså att skydd mot oönskad påverkan, ändring eller insyn säkras. Informationsägare ansvarar för att bedömning genomförs av om IT-avdelningens eller driftleverantörs standardrutiner för säkerhetskopiering är tillräckliga utifrån verksamhetens krav, eller om förstärkta åtgärder behövs i specifika fall. Informationsägare ansvarar även för att kontroll av återläsningens resultat avseende informationens riktighet utförs.

Kommunikationssäkerhet och informationsöverföring

Nätverk ska hanteras och styras för att skydda information i system och tillämpningar. Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller nätverkstjänster ska identifieras och inkluderas i avtal, oavsett om dessa tjänster tillhandahålls internt eller som en outsourcad tjänst. Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen av anslutna objekts krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.

Kontinuitet och avbrott

En kontinuitetsplan för kommunens IT-resurser och infrastruktur ska innehålla återstartsplaner för informationssystem och annan information som behövs om en allvarlig störning eller katastrof skulle inträffa.

Skydd mot skadlig kod

Upptäckande, förebyggande och återställande skydd mot skadlig kod i kommunens IT-miljöer ska finnas. Lämpliga rutiner ska införas för att uppmärksamma användarna på riskerna.

Hantering av tekniska sårbarheter;

Genomsökning och analys av tekniska sårbarheter i Värnamo kommuns IT-miljö ska ske löpande. Exponering för sårbarheter ska analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken. Det ska finnas rutiner så att information om tekniska sårbarheter erhålls i tid, att sårbarheter kan analyseras och lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför. För att uppnå spårbarhet och göra incidentutredningar möjliga ska kommunens IT-resurser och infrastruktur övervakas och loggas i den utsträckning som krävs. Detta för att förebygga, upptäcka och rätta till fel, oönskade händelser och förändringar i nätverk, IT- system och programvara, samt för att identifiera IT-incidenter och hot (exempelvis skadlig kod och intrångsförsök) mot kommunens utrustning, system eller information.

Dessa krav ska även beaktas avtalsmässigt vid köp av IT-tjänster av extern part, exempelvis molntjänster.

Säkra utrymmen för IT-resurser

Säkra utrymmen, såsom rum för servrar, switchar och annan kommunikationsutrustning, ska utformas så att utrustning inte utsätts för översvämning, brand, inbrott, sabotage eller andra händelser. Godkänt brandskydd och brandlarm ska finnas. Tillträden ska vara restriktiva och utifrån behov att i sin roll utföra uppdrag, samt styras och loggas via passersystem.

Kryptografiska säkerhetsåtgärder

Det ska finnas rutiner som beskriver hur kryptografiska säkerhetsåtgärder ska utvecklas och införas för skydd av information. Dessa rutiner ska också beskriva användning, skydd och giltighetstid för kryptologiska nycklar för hela deras livscykel.

Ansvarig

Kommundirektören.

Uppföljning

Riktlinjen ska ses över och uppdateras minst en gång per mandatperiod. Uppdatering åligger informationssäkerhetssamordnare.

Referenser

Andra relevanta interna styrdokument:

- Riktlinje för hantering av e-post i Värnamo kommun (2017-11-07)
- Riktlinje för hantering av personuppgifter i Värnamo kommun (2018-05-01)
- Riktlinje för mobila enheter och telefoni (2020-10-22)
- Riktlinje för distansarbete (2021-11-01)
- Riktlinje – Skrivare i Värnamo kommun (2021-11-24)