Sandvikens Kommun

Diarienummer
KS2024/181

» POLICY

Policy för IT- och informationssäkerhet

Styrdokumentets data

Beslutad av:	Kommunfullmäktige
Beslutsdatum och paragraf:	2024-04-15, § 43
Diarienummer:	KS2024/181
Giltighetstid:	Tills vidare
Dokumentansvarig:	Kommundirektör
För revidering ansvarar:	Chef för Kommunledningskontoret
För uppföljning och tidplan för denna ansvarar:	Chef för Kommunledningskontoret

Innehåll

Om denna policy

Policyn för IT- och informationssäkerhet har som syfte att fastställa Sandvikens kommunkoncerns övergripande viljeinriktning med IT- och informationssäkerhetsarbetet.

Policyn gäller för all IT- och informationssäkerhet i Sandvikens kommun och omfattar nämnder, medarbetare, förtroendevalda samt andra uppdragstagare – till exempel konsulter och praktikanter – som nyttjar Sandvikens kommuns informationstillgångar eller IT-system.

Om IT- och informationssäkerhet

Information finns i alla verksamheter inom Sandvikens kommunkoncern. Det kan vara information om medborgare, föreningar och företag eller om koncernens ekonomi och medarbetare. Information är i sig en av Sandvikens kommunkoncerns viktigaste tillgångar och för att nå hög kvalité och en väl fungerande verksamhet behöver information hanteras på rätt sätt och få rätt skydd.

Informationssäkerhet begränsas inte till frågor som rör IT utan handlar om skydd för alla informationstillgångar. Informationstillgångar kan exempelvis vara pappersdokument, flyttbara medier, telefoner eller IT-system. Information utgörs inte bara av text utan kan även vara i form av ljud, bild och film.

IT-säkerhet handlar om att skydda verksamhetens IT-relaterade tillgångar, som maskinvara, programvara och den information som lagras och hanteras i dessa.

Syfte med IT- och informationssäkerhet

IT- och informationssäkerhetsarbete innebär att skapa förutsättningar för att hantera information på rätt sätt och ge informationen rätt skydd i syfte att säkerställa informationens konfidentialitet, riktighet och tillgänglighet.

Ett kontinuerligt och systematiskt IT- och informationssäkerhetsarbete leder till att

- händelser som kan leda till negativa konsekvenser förebyggs
- uppdrag inom Sandvikens kommunkoncern kan genomföras utan störningar
- skapa motståndskraft och återhämtningsförmåga i de fall störningar ändå inträffar
- Sandvikens kommun har en ändamålsenlig, säker och robust drift och hantering av information och IT-system
- Sandvikens kommunkoncern möter medborgares, företags och andra aktörers förväntningar på säkerhet, integritet samt digital service
- ett högt förtroende för Sandvikens kommunkoncern upprätthålls
- IT- och informationssäkerhet är en naturlig och integrerad del i verksamheten.

Ansvar och roller

Ansvar och mandat med avseende på IT- och informationssäkerhet utgår från det ordinarie verksamhetsansvaret. Alla i Sandvikens kommunkoncern är utifrån sitt uppdrag ansvarig för sin del av IT- och informationssäkerheten.

Oavsett om det gäller förtroendevalda, medarbetare, uppdragstagare eller annan typ av användare är det viktigt att alla förstår sitt ansvar. Det är viktigt att alla användare är medvetna om hot och utmaningar som rör IT- och informationssäkerhet samt följer kommunens planer och informationsmaterial för IT- och informationssäkerhet vid utförande av sitt vardagliga arbete och för att minska risken för mänskliga fel.

Nedan listas för informationssäkerhetsarbetet centrala roller med tillhörande ansvar.

Kommunfullmäktige fastställer kommunens policy för IT- och informationssäkerhet.

Kommunstyrelsen har ett övergripande ansvar för kommunens interna säkerhetsfrågor och samordnar arbetet med IT- och informationssäkerhet samt verkar normerande, stödjande och uppföljande i relation till Sandvikens kommunkoncerns samtliga verksamheter.
Kommunstyrelsen är även Sandvikens kommuns arkivmyndighet. Detta innebär bland annat att tillse att myndigheternas allmänna handlingar hålls ordnade så att rätten att ta del av dem underlättas samt att handlingarna skyddas mot förstörelse, skada, tillgrepp och obehörig åtkomst. Kommunarkivet står för utförandet av detta uppdrag.

Nämnder och bolagsstyrelser äger och ansvarar för sina informationstillgångar och att de är förtecknade och klassificerade. De ansvarar även för IT- och informationssäkerheten inom sitt ansvarsområde samt att policyn efterlevs i verksamheten.

Chefer ansvarar för att IT- och informationssäkerhetsarbetet bedrivs i linje med policyn och rutiner/instruktioner inom sina respektive ansvarsområden.

Dataskyddsombudet granskar verksamheternas efterlevnad av dataskyddslagstiftningen samt ger råd och vägledning.

Dataskyddssamordnare ska utses på varje förvaltning och bolag. Denne ska samordna förvaltningens/bolagets arbete med att säkerställa att behandlingen av personuppgifter följer Dataskyddsförordningens krav. Det innebär till exempel att hjälpa till med att tillgodose de registrerades rättigheter och upprätthålla register över personuppgiftsbehandlingar, utreda incidenter och delta vid konsekvensbedömningar.

*Informationssäkerhetssamordnare a*nsvarar för övergripande samordning av informationssäkerhetsarbetet och granskar att denna policy följs. Informationssäkerhetssamordnaren ska också ge stöd, råd och vägledning till verksamheterna.

IT-säkerhetsansvarig ansvarar för övergripande samordning av IT-säkerhetsarbetet och granskar att denna policy följs. IT-säkerhetsansvarig ska också ge stöd, råd och vägledning till verksamheterna.

Medarbetare, förtroendevalda och andra användare avser den målgrupp till vilket det här dokumentet delvis är riktat till. Med användare menas den som på något sätt använder sig av de digitala verktyg som tillhandahålls av Sandvikens kommun. Ska följa policys, planer och instruktioner för IT- och informationssäkerhet.

Objektägare har det övergripande ansvaret för förvaltningsobjekt. Förvaltningsobjekt är ett ansvarsområde som definierar efter organisationens huvudprocesser[1]. IT-objekt ska uppfylla IT- och informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav.

Objektledare ansvarar för att systemet hålls uppdaterat och håller sig uppdaterad på de risker och sårbarheter som finns. Ansvarar även för att rutiner för behörighetsstyrning finns och följs.

Informationsägare Har det yttersta ansvaret för informationen. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem. Ställer krav på säkerheten för informationen. Informationsägare är vanligtvis nämnd eller bolagsstyrelse men det kan även finnas en utpekad roll eller befattning inom förvaltningsorganisationen som är informationsägare.

IT-chef Har det övergripande ansvaret för att uppfylla de krav som ställs på den tekniska IT-infrastrukturen samt att se till att aktuella regler och instruktioner finns för användning av kommunens IT-system och arbetsenheter.

Styrning och uppföljning

Nämnderna och bolagsstyrelserna ska säkerställa att IT- och informationssäkerhetspolicyn efterlevs. Kommunstyrelsen ska årligen följa upp läge och status. Särskilda skäl som allvarliga incidenter och brister kan motivera ytterligare uppföljningar.

IT- och informationssäkerhetsarbetet

Informationssäkerhetsanalys och handlingsplaner

Vartannat år ska kommunstyrelsen genomföra en IT- och informationssäkerhetsanalys i Sandvikens kommun. Analysen innefattar hot- och riskbild, skyddsnivåer, kommunens inriktning och interna och externa krav. Analysen ligger till grund för hur arbetet med IT- och informationssäkerhet ska bedrivas.

Identifiering, förteckning och klassificering

All information ska vara identifierad och förtecknad i nämndens informationshanteringsplan/dokumenthanteringsplan.

[1] Ett förvaltningsobjekt innehåller en eller flera informationsbärare, till exempel IT-system eller annan digital informationsbärare men det kan även röra sig om analoga informationsbärare som pärmar och arkivskåp.

Samtliga verksamhetssystem ska vara beskrivna och klassade i kommunens system för objektförvaltning och informationssäkerhet. Av förteckningen ska framgå vem som är informationsägare och i förkommande fall objektägare.

Det är varje nämnds ansvar att ha sina informationstillgångar förtecknade.

Informationsklassificering är en grundläggande del i arbetet med systematisk IT- och informationssäkerhet. Genom att klassificera information utifrån aspekterna konfiendialitet, riktighet och tillgänglighet kan rätt skydd ges till informationen.

Riskhantering och riskanalys

I samband med att informationstillgångar klassificeras ska en riskanalys genomföras. Syftet är att identifiera tänkbara störningar och allvarliga händelser för att kunna arbeta med förebyggande åtgärder. Detta syftar till att ha en säker informationshantering samt till att ha robusta informationstillgångar. IT- och informationssäkerhetsarbetet ska fokusera på förebyggande insatser, konkreta skyddsåtgärder och ständiga förbättringar.

Riskanalys ska genomföras i samband med större förändringar i eller omkring en informationstillgång. Riskanalys ska kontinuerligt genomföras för verksamhetskritiska informationstillgångar och/eller tillgångar som innehåller känslig information.

Skyddsnivå hos informationstillgångar

Alla informationstillgångar inom kommunen ska ha ett anpassat skydd så att informationens konfidentialitet, riktighet och tillgänglighet upprätthålls. Skyddsnivån för informationstillgångarna ska utformas så att fel, obehörig förändring, missbruk eller andra incidenter förhindras.

Utbildning

Medarbetare, förtroendevalda och andra användare ska få den utbildning som krävs för att kunna hantera information och system på rätt sätt.

Alla nyanställda och nytillträdda förtroendevalda inom Sandvikens kommunkoncern ska genomföra Sandvikens kommuns IT-introduktionsutbildning.

IT-säkerhetsansvarig och informationssäkerhetssamordnare ska återkommande genomföra olika IT- och informationssäkerhetshöjande insatser och utbildningar.

Behörighet och åtkomst

Medarbetare, förtroendevalda och andra användare i Sandvikens kommun ska ha ett personligt användarkonto för åtkomst till kommunens nätverk och IT-stöd då de utgör en del av kommunens informationstillgångar. Det innebär att det inte är tillåtet att lämna ut användaruppgifter Användare får inte heller nyttja en annan användares konto.

Beställning av behörigheter

Behörighetsnivå styrs av vilka arbetsuppgifter/vilken roll användaren har och vilken information vederbörande behöver för att utföra sina arbetsuppgifter.

Användare ska inte ha tillgång till mer information än vad som är nödvändigt för att utföra sina arbetsuppgifter.

I vissa roller ska det säkerställas att den anställde är lämplig för sin roll i syfte att minska risken för stöld, bedrägeri eller missbruk av resurser.

För att få tillgång och behörigheter till nätverk och eventuella verksamhetssystem behöver användarens chef godkänna samt beställa detta genom IT-kontoret eller objektledare. Beställning av behörigheter för förtroendevalda hanteras av den administrativa enheten vid kommunledningskontoret.

Avslut av behörigheter

Oavsett om det gäller en medarbetare, uppdragstagare eller annan typ av användare ska vederbörandes närmaste chef vid ändrat anställningsförhållande säkerställa att användarkonto samt behörigheter justeras eller avslutas för medarbetaren. Ändring och avslut av behörigheter för förtroendevalda hanteras av den administrativa enheten vid kommunledningskontoret.

Bearbetning lagring och förmedling av information och data

Information behöver olika typer av skydd, det kan vara tekniskt, till exempel brandvägg i ett IT-nätverk eller administrativt i form av regler som denna policy eller fysiskt som hur man skyddar utrymmen med dörrar, lås eller skåp.

För information som hanteras, bearbetas, lagras och kommuniceras gäller följande:

- Hanteringen av information får inte bryta mot svensk lagstiftning.
- Samtliga användare ska hantera information i enlighet med de regler som finns.
- Samtliga användare har ett personligt ansvar för säkerheten i hantering av information i alla dess former.
- Handlingar som innehåller information som omfattas av sekretess eller känsliga personuppgifter[2] ska i första hand lagras i ett befintligt verksamhetssystem som är säkerhetsmässigt godkänt och i andra hand lagras på annan godkänd lagringsplats. Användare kan av sin chef få hjälp med att definiera vad som är känsliga personuppgifter eller vad som omfattas av sekretess[3]. Förtroendevalda kan kontakta kommunstyrelseförvaltningen för råd och stöd.

Den som använder kommunens informationstillgångar eller i övrigt agerar på ett sätt som strider mot styrdokument avseende IT- och informationssäkerhet kan bli föremål för arbetsrättsliga påföljder. Vid misstanke om brott görs polisanmälan.

[2] Känsliga personuppgifter kan till exempel vara politiska åsikter, etniskt ursprung, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter, biometriska uppgifter som används för att entydigt identifiera en person

[3] Regler om allmänna handlingars offentlighet samt om sekretess återfinns huvudsakligen i Tryckfrihetsförordningen (TF 1949:105) eller i Offentlighets- och eller sekretesslagen (2009:400).

Användning av IT-utrustning och internet

Medarbetare, förtroendevalda och andra användare som nyttjar Sandvikens kommuns nätverk och/eller datorer, mobila enheter och kringutrustning har ett personligt ansvar att följa de regler och instruktioner[4] som gäller och för nyttjandet av datorer och mobila enheter.

Användare gör sig skyldig till lagbrott eller regelbrott genom till exempel:

- olovligt intrång, försök eller förberedelser till intrång i informationstillgångar eller programvaror
- utlånande av användaridentitet eller utnyttjande någon annans, detta gäller även lösenordet och tjänstekort/passerkort som används vid inloggning
- att försöka dölja sin användaridentitet
- att sabotera eller manipulera nätverk, datorer eller kringutrustning
- att manipulera information i strid med gällande lagar och regler
- att radera information utan stöd i lag, dokumenthanteringsplan eller annat tillstånd
- att använda, kopiera eller distribuera upphovsrättsligt eller på annat sätt skyddat material om rättighetsinnehavaren inte har lämnat medgivande till detta

Vid överträdelse av lag eller regler av medarbetare eller uppdragstagare gällande IT- eller informationssäkerhet fattas eventuell åtgärd av behörig chef, i samråd med HR-funktion och IT-chef vid behov.

Vid överträdelse av lag eller regler gällande IT- eller informationssäkerhet av förtroendevalda fattas eventuell åtgärd av IT-chef och HR-chef i samråd.

Internetanvändare representerar kommunen och lämnar spår efter sig i form av kommunens IP-adress. Användningen av internet bör utföras med gott omdöme, detta för att undvika att användarens agerande på internet skadar kommunen.

Kontinuitetsplanering

Verksamheterna ska ha kontinuitetsplaner och rutiner för att kunna fullfölja sitt åtagande även vid exempelvis systemavbrott. Kontinuitetsplaner ska finnas för verksamheternas kritiska processer i syfte att säkerställa att viktiga funktioner kan ha minsta möjliga avbrottstid. Detta är även en viktig del i objektförvaltningsarbetet.

IT- och informationssäkerhetsincidenter

IT- och informationssäkerhetsincidenter ska utan dröjsmål rapporteras till IT-kontoret. Incidenterna ska dokumenteras och i förekommande fall anmälas till tillsynsmyndighet/-er eller polisanmälas då brott misstänks föreligga.

Fysisk säkerhet

Nivån på det fysiska skyddet ska stå i proportion till resultatet av informationsklassificeringarna och de återkommande riskanalyserna.

[4] IT-kontoret publicerar aktuella regler och instruktioner på intranätet

Utrustning som datorer, servrar, med mera och informationstillgångar ska skyddas mot förlust, skada, stöld eller liknande.

Kommunens serverhallar ska uppfylla höga krav på fysisk säkerhet. Inför utkontraktering (exempelvis vid användning av molntjänster) är det viktigt att kravställning på fysisk säkerhet sker i samband med anskaffningen.

IT-system

Anskaffning av IT-system

Inför anskaffning[5] av IT-system där information hanteras eller vid behov av ny funktionalitet är det viktigt att vid ett tidigt stadium undersöka om ett IT-system med motsvarande funktionalitet redan finns.
Den berörda verksamheten ska inför en anskaffning identifiera vilka behov verksamheten har, vilken information som ska hanteras och vilka lagkrav som omfattas. I samband med detta ska den berörda verksamheten genomföra en informationsklassificering och riskanalys med tillhörande åtgärdslista. Syftet med det är att rätt krav ska kunna ställas vid anskaffningen för att på så sätt ge informationen rätt skydd.

All anskaffning i Sandvikens kommun ska följa det samlade regelverket som finns för inköp (policy, riktlinje och handbok). Inför och vid anskaffning av IT-system ska inköpsenheten på ekonomikontoret alltid kontaktas.

Avveckling av IT-system

Inför avveckling av IT-system ska en plan för avveckling finnas. Vid avveckling är det viktigt att krav på gallring och arkivering beaktas. Informationen som gallras ska förstöras på ett sådant sätt att informationen inte kan återskapas, återläsas eller komma i orätta händer. Informationen kan även komma att migreras till ett nytt system.

[5] Med anskaffning menas bland annat upphandling, direktupphandling, inköp, avrop, uppgradering eller liknande.