Fastställd: Kommunfullmäktige 2026-06-04, § 79

Gäller för: Bollebygds kommun

Dokumentansvarig:
Informationssäkerhetssamordnare

Dnr : **KS2026/43-4**

Policy Informationssäkerhet, cybersäkerhet och dataskydd

Postadress	Besöksadress	Telefon	Telefax	Webbplats	E-post
517 83 Bollebygd	Ballebovägen 2	033–231300	033-231428	www.bollebygd.se	kommunen@bollebygd.se

Innehållsförteckning

Innehåll

Inledning

Denna policy redovisar Bollebygd Kommuns viljeinriktning och övergripande principer över informationssäkerhet, cybersäkerhet och personuppgiftshantering i kommunen. Policyn åskådliggörs i styrdokumentet Riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd.

Syftet med policyn är att klarlägga

- Mål
- Organisation, ansvar och roller
- Riktlinjer för områden av särskild betydelse

Information utgör en av de mest strategiska resurserna kommunen förfogar över. Alla verksamheter är beroende av tillförlitlig information där avbrott i tillgängligheten till den kan ge i allvarliga konsekvenser för medborgare, verksamheter och tredje part.

Kraven på informationssäkerhet utgår från kommunledningen och verksamhetens krav på funktion, relevans och legala krav, utöver detta även avtal och säkerhetskrav. Med lämplig, relevant och rätt informationssäkerhet kan en hög kvalitet och produktivitet uppnås i det dagliga arbetet. Det förebygger störningar, skapar kontinuitet och föreslår lämpliga åtgärder mot de risker som identifieras. Insatser utgår från verksamheternas behov och ska vara en del av kommunens totala riskhantering.

Kommunledningsgruppen fastställer vilka verksamhetsprocesser som är samhällsviktiga. Den information och de IT-system som stöder de informationsflödena ska på så sätt också betraktas som samhällsviktiga. Det medföljer en informationsklassning, risk-och sårbarhetsanalys, kontinuitetshantering som ska mynna ut och motsvara ett skydd som adresserar informationen och systemet som behandlas. Utgångspunkten är att informationsägaren ansvarar för att informationen hanteras på ett säkert och ändamålsenligt sätt

Kommunens förvaltningar ska i så stor utsträckning det är möjligt, följa etablerade standarder och vägledningar som baseras på Svensk Standard för Informationssäkerhet i enlighet med ISO/IEC 27000-serien.

Policyn ska, av chef eller motsvarande, kommuniceras till samtliga medarbetare och förtroendevalda. Den ska ingå i introduktionen vid nyanställning och vid nya uppdrag, samt när policyn revideras. Policyn ska vara känd och tillgänglig i sin aktuella version på kommunens intranät och på kommunens hemsida.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna policy.

Bakgrund

Information finns och behandlas i alla kommunens verksamheter, och som är beroende av att information är tillgänglig för rätt person vid rätt tidpunkt, att den är korrekt och riktig, och på så sätt utgör ett bra verksamhetsstöd, samt möjliggör för oss som organisation att uppfylla vårt uppdrag i samhället.

Det finns idag många hot mot våra informationstillgångar och för att säkerställa att informationen är skyddad finns det särskilda informationssäkerhetskrav som behöver uppfyllas. Informationssäkerhet avgränsas till skydd av informationstillgångar och tar sikte på nödvändig och adekvat nivå på sekretess, riktighet, tillgänglighet och spårbarhet.

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: att information är korrekt, aktuell och fullständig.
- Tillgänglighet: åtkomlighet för behörig person vid rätt tillfälle.
- Spårbarhet: härledning av utförda aktiviteter till en identifierad användare.

Delar av kraven kretsar kring medarbetares kunskap och vår organisationskultur kring informationssäkerhet. Det inkluderar utbildningar, övningar, processer och etablerade rutiner som stödjer ett säkert arbetssätt. Den delen betraktas som den mjuka sidan av informationssäkerheten och ställer krav på organisationens chefer att säkerställa att medarbetare genomför utbildningar, följer gemensamma processer och tillämpar säkerhetsrutiner i det dagliga arbetet.

Den del som kan betraktas som den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. En viktig del är också revision och uppföljning.

Den tekniska säkerheten beskrivs även som IT-säkerhet. Häri återfinns nätverk, servrar, arbetsstationer, hård-och mjukvara samt serverrum. Här finns även reservkraft, säkerhetskopior med mera.

Den sista delen är fysisk säkerhet, som till stor del hör ihop med den tekniska säkerheten. Den tar sikte på hur vi skyddar vår organisations materiel, system och personal rent fysiskt. Det innebär bland annat att kontrollera tillträde till lokaler, använda lås och larm samt se till att obehöriga inte får fysisk åtkomst till känslig utrustning. Fysisk säkerhet är en viktig del av informationssäkerheten och bidrar till att skydda informationens konfidentialitet, riktighet och tillgänglighet.

Om personuppgiftshantering

I många avseenden förekommer även personuppgifter i information som hanteras. Personuppgifter står under särskilt skydd och råder under särskilda bestämmelser enligt Dataskyddsförordningen (GDPR) samt nationell kompletterande lag; Dataskyddslag. För personuppgifter gäller således särskilda regler för hantering. Inom ramen för informationssäkerhet är det viktigt att identifiera personuppgifter som särskilt skyddsvärda samt ändamålsenligt hanterade.

GDPR säger att personuppgifter bara får användas om det finns lagligt stöd för det. Det kan till exempel vara ett avtal, en lag eller att personen har sagt ja (gett sitt samtycke). Förordningen gäller oavsett om uppgifterna hanteras digitalt eller på papper, den är teknikoberoende. Medarbetare i Bollebygds Kommun som arbetar med personuppgifter måste veta hur man skyddar dem på ett säkert sätt, så att ingen obehörig kan komma åt dem.

Omfattning och principer

Policyn är normerande, stödjande och kontrollerande och gäller all verksamhet inom Bollebygds kommun och omfattar alla informationstillgångar som kommunen hanterar. Den beskriver hur vi ska arbeta för att skydda information på ett enhetligt och säkert sätt. Policyn ger vägledning i det

dagliga arbetet och tydliggör vilket ansvar olika roller har när det gäller att hantera information korrekt.

Den innebär att samtliga medarbetar, förtroendevalda, elever och inhyrd personal omfattas av policyn och dess tillhörande rutiner. Alltså, den gäller för alla som brukar kommunens informationstillgångar på ett sådant sätt att de kan påverka informationens sekretess, riktighet, och/eller tillgänglighet.

Informationstillgång definieras som all information, oaktat om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock som i ett samtal. Film, ljud och bild omfattas också av informationssäkerhetsbegreppet.

Det övergripande målet är enkelt uttryckt att rätt information ska vara tillgänglig för rätt person i rätt tid. Detta beskrivs mer detaljerat i Riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd.

Riskhantering

Kommunen har ett övergripande arbetssätt som utgår från en allriskansats och omfattar systematisk riskidentifiering, riskbedömning och riskhantering. Arbetet med informations- och cybersäkerhet är en central del av det systematiska säkerhetsarbetet och utformas i enlighet med kraven i NIS-2-direktivet, Dataskyddsförordningen (GDPR), CER-direktivet och annan väsentlig lagstiftning.

Målet är att stärka organisationens förmåga att förebygga, motstå, hantera och återhämta sig från incidenter som kan påverka informationssäkerheten, kontinuiteten i samhällsviktiga tjänster samt skyddet av personuppgifter. Riskhantering bedrivs kontinuerligt, integrerat i verksamhetsstyrningen och inom ramen för de mandat som respektive förvaltning besitter.

Mer detaljerad beskrivning av arbetssätt, roller och ansvar återfinns i tillhörande riktlinjer.

Incidenthantering

I kommunens finns det en dokumenterad process för hantering av informationssäkerhets- och personuppgiftsincidenter. Syftet är att möjliggöra

tidig upptäckt, korrekt rapportering, effektiv hantering och lärande efter incident. Processen omfattar bland annat:

- Intern rapportering enligt gällande rutin samt till närmsta chef, informationssäkerhetssamordnaren, IT-enhetschef och eventuellt dataskyddsombud.
- Bedömning av incidentens allvarlighetsgrad och påverkan.
- Rapportering till tillsynsmyndighet vid allvarliga incidenter i enlighet med NIS2 (inom 24 timmar) och GDPR (inom 72 timmar).
- Återställning av verksamhet och informationssystem.
- Dokumentation, analys och förbättringsåtgärder.

Mer detaljerade instruktioner och anvisningar återfinns i kommunens riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd.

Ledningssystem för informationssäkerhet (LISD)

Den samlade dokumentationen tillsammans med de processer som ingår i ett systematiskt informationssäkerhetsarbete, utgör ett ledningssystem för Informationssäkerhet, cybersäkerhet och dataskydd, (LISD).
Ledningssystemet bygger på standarden för ledningssystem för informationssäkerhet ISO/IEC 27001, GDPR samt dataskydds-förordningen.
Informationssäkerhetsarbetet är uppbyggt på samma sätt som andra former av systematiskt kvalitetsarbete. Det bygger på en tydlig och återkommande cykel där kommunen planerar, genomför, följer upp och förbättrar. Inom LISD innebär det att arbetet sker strukturerat och kontinuerligt, med löpande mätning, analys och justering av kommunens skyddsåtgärder. På så sätt säkerställer man att informationssäkerhet, cybersäkerhet och dataskydd hela tiden utvecklas och håller rätt nivå över tid.

Efterlevnaden av informationssäkerhetspolicy, riktlinjer för informationssäkerhet och
riktlinjer för personuppgiftshantering ska regelbundet följas upp.

Informationssäkerhetssamordnare ska rapportera läge och status gällande informations-säkerhet till kommunstyrelsen där rapporteringen ska ske en gång per år. Om särskilda skäl finns, som exempelvis vid allvarliga incidenter, brister eller behov, ska det motivera ytterligare rapporteringar.

Organisation, roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att information och tjänster kan administreras och hanteras på ett sådant sätt att de under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål.

All information ska klassificeras utifrån verksamhetens krav på konfidentialitet, riktighet och tillgänglighet. Den information som omfattas av sekretess enligt lag, är personuppgifter eller är relaterade till personuppgifter ska även klassas utifrån krav på spårbarhet. Det ska förtecknas vilken klassificering en informationsmängd har. All hantering, bearbetning och lagring av information skall motsvara kraven i dess klassning.

Kommunfullmäktige är ytterst ansvarig för informationssäkerhets- och dataskyddsarbetet och uttrycker sin viljeinriktning i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informations-säkerhets- och dataskyddsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd.

Varje nämnd med förvaltning ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras. Enligt dataskyddsförordningen är det den som ansvarar för personuppgifterna som också har ansvaret. Det innebär att varje nämnd själv bär det fulla ansvaret för att all behandling av personuppgifter inom den egna verksamheten sker i enlighet med dataskyddsförordningens krav och grundprinciper.

Policyn för informationssäkerhet, cybersäkerhet och dataskydd gäller för alla informations-tillgångar och personuppgiftsbehandlingar i alla verksamheter

inom kommunen. Policyn gäller för samtliga aktörer som kan komma att hantera kommunens information och personuppgifter.

Personer som hanterar information och personuppgifter ska ha kunskap om gällande regelverk för hur dessa får behandlas. De har själva ett ansvar för att informationssäkerhet, cybersäkerhet och dataskydd upprätthålls. Vid upptäckt av incidenter eller brister ska incidentrapportering ske enligt fastställd rutin.

Andra viktiga roller inom informations- och IT-säkerhetsarbetet är systemägare, objektägare, informationsägare och systemförvaltare. I de flesta fall är informationsägaren även riskägare, vilket betyder att personen eller funktionen ansvarar för att identifiera och hantera de risker som framkommer i risk- och sårbarhetsanalyser.

Uppföljning

Kommunstyrelsen och kommunledningsgruppen ska minst en gång per år informera sig om arbetet med informationssäkerhet, cybersäkerhet och dataskyddet. Denna uppföljning ska baseras på underlag med rekommendationer som tas fram av informationssäkerhets-samordnaren. Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten
- Utbildning (status och behov)
- Inträffade incidenter
- Resultat från genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till förbättringar
- Genomförda riskanalyser

Resultatet från denna uppföljning ska innefatta förslag till beslut om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser.

Uppföljning ska årligen genomföras för att kontrollera att tekniken fungerar utifrån de säkerhetskrav som finns, samt att regler efterlevs. Ansvarig för

uppföljningen är kommunens informationssäkerhetssamordnare. Genomförandet kan delegeras.

Ifall misstanke om oegentlighet uppstår ska detta utan fördröjning anmälas till närmsta chef. I de fall regler inte följs kan följden bli disciplinära åtgärder. Om man kan förmoda att brott mot lag har begåtts lämnas information till brottsutredande myndighet.