Informationssäkerhet och dataskydd, riktlinjer

Dokumenttyp	Riktlinjer
Fastställd/upprättad	Kommunstyrelsen 2026-05-06, § 52
Senast reviderad	
Detta dokument gäller för	Kommunövergripande
Giltighetstid	Tills vidare
Dokumentansvarig	Kommundirektör
Dnr	2026-136

Innehåll

Informationssäkerhet och dataskydd

Dessa riktlinjer förtydligar kommunfullmäktiges policy för systematiskt informationssäkerhetsarbete inom arbetsområdena informationssäkerhet och dataskydd.

Riktlinjerna styr:

- Hur förvaltningen ska anordna sitt riskbaserade, systematiska informationssäkerhetsarbete.
- Vad förvaltningen ska göra för att skapa förmåga hos alla anställda och politiker att upprätthålla informationssäkerheten och dataskyddet i förvaltningen.
- Vad förvaltningen ska vidta för åtgärder för att utveckla och anpassa informationssäkerhetsarbetet samt dataskyddet.
- Vad förvaltningen ska vidta för åtgärder för att skydda verksamhet och information från negativ påverkan från identifierade risker och hot.

Ansvar och uppgifter

Kommundirektören ska:

- tillse att förvaltningen arbetar för och efterlever riktlinjerna.
- tillse att kommunstyrelsen hålls underrättad om hur arbetet med att uppfylla riktlinjerna går och vilka resursbehov som finns för att tillmötesgå dem. Information ska ske årligen och finnas dokumenterad.
- fördela arbetet som syftar till att leva upp till riktlinjerna på lämpligt sätt i förvaltningen och som inkluderar roller i förvaltningsledningen, strategiska befattningar och verksamheterna.

Krav på arbetssätt

Nedan listas de krav som ställs på förvaltningens arbete med informationssäkerhet och dataskydd.

Systematiskt arbetssätt

- Förvaltningen ska bedriva systematiskt arbete inom informationssäkerhet och dataskydd, samordnat och direkt styrt av kommundirektören och kommunledningen.
- Varje område ska ha beslutande (chef) och samordnande (handläggare) roller.
- Arbetsmetoden ska utgöras av rutinbaserat arbete; utbildning, administration, återkommande aktiviteter på årsbasis och riskbaserade åtgärder i hela förvaltningen.
- Arbetsmetoden ska inkludera årliga uppföljningar och kontroller av systematiken, informationssäkerheten och dataskyddet samt inkludera kostnadssammanställningar för den genomförda verksamheten.

- Arbetsmetoden och åtgärder som vidtas ska vara kunskapsbaserade och grunda sig i regelbundet uppdaterade risk- och sårbarhetsanalyser, uppföljning av arbetet och incidentrapportering som förvaltningen sammanställt.
- Information ska vara klassad utefter hur viktig den är för verksamheten och säkerhetsåtgärder och arbetssätt utformade därefter.
- Det systematiska arbetet med informationssäkerhet och dataskydd ska vara närvarande i alla processer och områden där information hanteras; lagras eller bearbetas. Både digitalt och analogt.
- Förvaltningen ska bedriva den omvärldsbevakning som krävs för att hålla sig informerad om gällande bestämmelser inom informationssäkerhets och dataskydd. Omvärldsbevakningen ska särskilt fokusera på nationella samordnings- och tillsynsmyndigheters information och kommunikation inom cybersäkerhet.

Förmåga till informationssäkerhet och dataskydd genom utbildning

- Alla anställda och politiker ska få regelbunden, relevant och verksamhetsnära utbildning som höjer kommunens förmåga att bedriva informationssäkerhets- och dataskyddsarbete. Det inkluderar ett introduktionsprogram för informationssäkerhet och dataskydd.
- Förvaltningen ska bedriva användarvänlig och tillgänglig introduktion av politiker och anställda inom informationssäkerhet och dataskydd.
- Förvaltningen ska underhålla rutiner och instruktioner i lämpligt format för att vägleda och instruera i *hur* arbetet ska bedrivas, i syfte att skapa medvetenhet och motivera den enskilde att agera säkert.
- Förmågan i förvaltningen ska utvärderas och följas upp regelbundet så att brister åtgärdas snabbt.

Utveckling och anpassning av informationssäkerhetsarbetet och dataskyddet

- Förvaltningen ska bedriva den omvärldsbevakning, samverkan och internt arbete som krävs för att hålla informationssäkerhetsarbetet och dataskyddet relevant och ändamålsenligt, samt förenlig med nationella lagar, regler och föreskrifter samt den dagliga verksamheten.
- Förvaltningen ska systematiskt utvärdera störningar, incidenter och andra händelser som kan påverka informationssäkerhetsarbetet och dataskyddet. Slutsatserna från utvärderingarna ska integreras i det systematiska arbetet.
- Vid inköp av tjänster eller hårdvara ska det tas hänsyn till informationssäkerheten och dataskyddet. Det innebär att det ska ställas relevanta krav på leverantör och utrustning innan den upphandlas och tas i drift.

Skydd av verksamhet och information mot hot och risker

- Skyddet av kommunens verksamheter ska dimensioneras baserat på identifierade hot, risker och sårbarheter.

- Förvaltningen ska regelbundet följa upp vilka störningar, avbrott och incidenter som skett i den egna verksamheten. Baserat på uppföljningen ska förvaltningen utvärdera befintliga säkerhetsåtgärder och rutiner.
- Det ska finnas tydliga informations- och rapporteringsvägar vid interna händelser som ska nyttjas för att informera den del av förvaltningen som ska leda hanteringen.
- Hanteringen av händelser och incidenter som har omfattande påverkan på verksamheten ska hanteras som en fredstida kris (extraordinär händelse), och med motsvarande resurser som hade blivit ianspråktagna vid andra typer av fredstida kriser.
- Förvaltningen ska hantera personuppgifter på ett sådant sätt att de registrerades fri- och rättigheter garanteras och integriteten skyddas. Arbetet ska utgå ifrån dataskyddsförordningen och omsättas att passa förvaltningens arbetssätt.

Incidenthantering i övrigt

- Förvaltningen ska ha kännedom om vilka incidenter som inträffar i den dagliga verksamheten.
- Varje konstaterad och inrapporterad incident, oavsett omfattning eller typ, ska dokumenteras.
- Förvaltningen ska tillhandahålla användarvänliga och snabba rapporteringssätt för anställda och politiker.
- Kopplat till rapporteringen ska förvaltningen ha en planerad och övad incidenthanteringsprocess och organisation.
- Alla incidenter ska förutom ovan, rapporteras till de myndigheter som ansvarar för dataskydd och cybersäkerhet och följa dessas föreskrifter om innehåll och omfattning.

Personalsäkerhet

- Endast behörig och utbildad personal får nyttja kommunens informationstillgångar eller beredas tillgång till de miljöer där information hanteras, förvaras eller finns tillgänglig. Undantag gäller de allmänna handlingar som ska finnas öppet tillgängliga.
- Informationstillgångar och system där dessa förvaras och hanteras ska genom informationsklassning beläggas med säkerhetsåtgärder som styr behörigheter och tillgänglighet.
- Konsulter och inhyrd personal som till vardags inte ingår i kommunens organisation men behöver ha tillgång till information och IT-resurser ska utbildas innan de får tillgång.
- Extern servicepersonal ska kontrolleras så att identiteter överensstämmer med det som angivits vid bokning av servicen. Dessa ska ledsagas genom kommunens lokaler och då de befinner sig i utrymmen för känslig eller kritiska informations- eller systemresurser.

- Extern personals tillgång till och verksamhet i IT-miljöer i utbildnings-, utvecklings- eller serviceärenden ska loggas och spåras.

- Extern personal ska vid risk för eller direkt tillgång till information eller verksamhet som omfattas eller kan antas omfattas av sekretess, på förhand underteckna en sekretesserinran och informeras om eventuell tystnadsplikt.

- Med extern personal menas personal som inte är anställda av Hjo kommun.

Återrapportering och uppföljning

Förvaltningens uppföljning

Varje år ska förvaltningen följa upp informationssäkerheten och dataskyddet samt det systematiska arbetet. Dokumentationen därifrån ska vara strukturerad och enhetlig.

Varje uppföljning i respektive område ska vid behov kunna redovisas till kommunstyrelsen separat från den övriga årliga redovisningen.

Årlig återrapportering

Det pågående arbetet, inklusive slutsatser och en bedömning av huruvida dessa riktlinjer följs, ska redovisas till kommunstyrelsen.

Förvaltningen bör samordna uppföljningen med andra relaterade uppföljningar som sker årligen.

Följande rubriker ska inkluderas i den årliga återrapporteringen:

- *Genomförda åtgärder*, med hänvisning till risker som påverkats och mål i policyn som berörs.

- *Inträffade incidenter och händelser*, vilka åtgärder som vidtagits och övergripande slutsatser av händelserna, hanteringen och dess konsekvenser. Det ska också framgå hur liknande, framtida incidenter förebyggs.

- *Status per områd*e, sammanfattning av uppföljningen och kontrollen av respektive område. Hur arbetet fortskrider, utmaningar och problem samt framgångsfaktorer och positiva effekter.

- *Budgetsammanställning* för det gångna årets utgifter; uppskattade personalkostnader (arbetstid) för arbetet (investeringar och åtgärder), incidenthantering och kostnader som inte varit budgeterade. Dessa ska vara förklarade och motiverade under denna rubrik.

- Sådant som varit budgeterat ska redovisas mot den faktiska kostnaden, t.ex. systemanskaffningar och andra investeringar men också underhållskostnader.

Ovan ska inte innehålla sekretessbelagda uppgifter. Data och underlag till rapporten som är sekretessbelagda ska finnas tillgängliga för särskild granskning vid behov.

Återrapportering i slutet på mandatperioden

I slutet av varje mandatperiod ska förvaltningen sammanfatta innevarande mandatperiods genomförda arbete och redovisa hur policyn och riktlinjen omsatts i förvaltningen. Redovisningen ska ske skriftligt och presenteras muntligt i kommunstyrelsen.

Följande rubriker ska inkluderas i redovisningen i slutet på varje mandatperiod:

- *Beskrivning av det genomförda arbetet*; redovisning för hur inriktningen följts.
- *Hanterade risker*; vilka risker ur risk- och sårbarhetsanalysen som har hanterats genom åtgärder och hur riskbilden bedömts har påverkats.
- *Antal incidenter per område*; informationssäkerhet och dataskydd.
- *Slutsatser kring arbetet*, vad har fungerat som det ska, vad har inte fungerat som det ska, har policy och riktlinjer kunnat följas?
- *Budget*, hur har kostnadsbilden sett ut per år under mandatperioden, hur har den varierat och hur har åtgärder påverkat den.

Ovan ska inte innehålla sekretessbelagda uppgifter. Data och underlag till rapporten som är sekretessbelagda ska finnas tillgängliga för särskild granskning vid behov.