HJO

# IT och IT-säkerhet, riktlinjer

| | |
|---|---|
| Dokumenttyp | Riktlinjer |
| Fastställd/upprättad | Kommunstyrelsen 2026-05-06, § 53 |
| Senast reviderad | |
| Detta dokument gäller för | Kommunövergripande |
| Giltighetstid | Tills vidare |
| Dokumentansvarig | Kommundirektör |
| Dnr | 2026-137 |

# Innehåll

# IT och IT-säkerhet

Dessa riktlinjer förtydligar kommunfullmäktiges policy för systematiskt informationssäkerhetsarbete inom arbetsområden IT och IT-säkerhet samt systemförvaltning.

Riktlinjerna styr:

- Hur förvaltningen ska anordna sitt riskbaserade, systematiska IT och IT-säkerhetsarbete samt systemförvaltning.
- Vad förvaltningen ska vidta för åtgärder för att utveckla och anpassa IT och IT-säkerhetsarbetet samt systemförvaltningen.
- Vad förvaltningen ska vidta för åtgärder för att skydda verksamheten och IT-miljön 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 i verksamheterna.

## Krav på arbetssätt

Nedan listas de krav som ställs på förvaltningens arbete med IT och IT-säkerhet.

*Systematiskt arbetssätt*

- Förvaltningen ska bedriva systematiskt arbete inom IT-säkerhet, IT-drift och systemförvaltning, samordnat och direkt styrt av kommundirektören och kommunledningen.
- Förvaltningen ska underhålla rutiner och instruktioner i lämpligt format för att vägleda och instruera i *hur* arbetet ska bedrivas.
- Arbetsområdet 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, IT-säkerheten, IT-driften och systemförvaltning samt inkludera kostnadssammanställningar för verksamheten.
- Arbetsmetoden och åtgärder som vidtas ska vara kunskapsbaserade och grunda sig i

regelbundet uppdaterade behovsanalyser och för IT-säkerheten risk- och sårbarhetsanalyser, uppföljning av arbetet och incidentrapportering som förvaltningen sammanställt.

- Förvaltningen ska bedriva den omvärldsbevakning som krävs för att hålla sig informerad och uppdaterad om nationella föreskrifter och regler som berör IT-säkerhet och kontinuitetskrav för IT. Bevakning ska minst utgå ifrån bevakning av nationella myndigheters kunskapsinstanser.

*Systemförvaltning och kontinuitet*

- Förvaltningen ska förvalta befintliga system och IT-lösningar som köpts in av externa leverantörer genom att underhålla noggranna register över de system och digitala verktyg som används. Dessa register ska hållas uppdaterade och deras riktighet följas upp.
- I sammanställningen av system och digitala tjänster ovan ska samtliga kostnader för tjänsterna redovisas.
- Förvaltningen ska tillse att det finns arbetsmetoder som vägleder hur systemens och tjänsternas långsiktiga finansiering och resurseffektivitet tillgodoses.
- Förvaltningen ska ha god kännedom om leverantörer och underleverantörer till system och tjänster och utreda hur dessa påverkar IT-säkerhet, dataskydd och informationssäkerheten.
- Externa leverantörers IT- och informationssäkerhetsarbete som kravställts av kommunen ska följas upp samt brister åtgärdas så snabbt som möjligt.
- Avtal om kritiska IT-system eller tjänster ska vara utformade att ställa krav på IT-säkerhet, informationssäkerhet, spårning, loggning och kontinuitet i fredstida händelser samt under höjd beredskap. Friskrivning av detta ska normalt inte tillåtas.
- Kravställning enligt föregående punkt gäller även om kommunen deltar i gemensamma upphandlingar med andra kommuner.
- Den verksamhet i förvaltningen som i huvudsak ska nyttja ett IT-system ska vara ansvarig för systemförvaltningen och att kommunens rutiner för systemförvaltning m.fl. samt dessa riktlinjer följs.
- Systemägare beslutar om säkerhetsåtgärder, kontinuitetsplaner och tecknar avtal samt ansvarar för systemens finansiering. Systemägare utses av respektive verksamhet eller kommundirektören.
- Förvaltningen ska genomföra systemklassning av samtliga IT-system där informationsklassning för den information som hanteras i respektive system blir vägledande för IT-systemens säkerhetsåtgärder och kontinuitetskrav. Vidare ska systemklassningen utreda konsekvenserna verksamheten drabbas av vid ett bortfall av funktionaliteten i systemet.

- Alla kritiska IT-system som behövs för att upprätthålla kommunens funktionalitet och samhällsviktiga verksamhet ska ha dokumenterade och implementerade

reservförfaranden och/eller kontinuitetsplaner.

- Alla kritiska IT-system och resurser ska av förvaltningen ha beslutade, accepterade avbrottstider varefter kontinuitetsplaner och nöddrift ska aktiveras.
- Alla kritiska IT-system ska av kommunledningen vara ordnande i en prioriteringsordning för återställning vid ett omfattande avbrott eller störning som omfattar flera IT-system samtidigt.

*Daglig IT-drift och samverkan*

- Alla anställda, politiker och personer som nyttjar kommunens IT ska få regelbunden, relevant och verksamhetsnära utbildning som underhåller kommunens förmåga till säkert och resurseffektivt nyttjande av IT (system och utrustning).
- Förvaltningen ska ha regelbunden samverkan med externa leverantörer om IT-drift och IT-säkerhet. Samverkan ska ha en förebyggande roll i att skapa framförhållning för utveckling av IT-infrastrukturen och förutsäga investeringsbehov.
- Kostnaderna för IT, säkerhetsåtgärder, underhåll av utrustning, konsultkostnader samt andra relaterade, löpande utgifter ska finnas väldokumenterade och tillgängliga för granskning.

*Utveckling och anpassning av IT*

- IT i sin helhet ska vara relevant och ändamålsenligt utformad för att effektivisera förvaltningens arbete samt vara användarvänlig för politiker och anställda.
- Förvaltningen ska genom utbildning och interna aktiviteter vägleda och möjliggöra verksamheternas IT-användning genom att anpassa dess utformning och användningsområden till verksamheternas behov. Det inkluderar tillgängligheten på IT för politiker och anställda.
- Förvaltningen ska systematiskt utvärdera störningar, incidenter och andra händelser som påverkar IT-säkerheten. Slutsatserna från utvärderingarna ska integreras i det systematiska arbetet och ligga till grund för utvecklingen av miljöerna.

*IT-säkerhet och incidenthantering*

- 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.

- Vid allvarliga avbrott, störningar eller attacker inom IT, som skadar kommunens verksamhet och service till samhället, ska rapportering ske till nationella instanser så som dessa myndigheter föreskriver det. Kommunen ska ha välförankrade rutiner som

möjliggör sådan rapportering.

- Förvaltningen ska tillse att det finns tydliga krav vid upphandling och inköp av system och digitala tjänster när det gäller IT-säkerhet och tillgänglighetsanpassning, som följer nationella regler och föreskrifter. Detta ska ske samordnat med informationssäkerhets- och dataskyddsarbetet.
- Kommunens IT ska ha behörighetsstyrning och säkerhetsfunktioner som försvårar obehörig tillgång.
- Förvaltningen ska ha rutiner som informerar om avbrott, störningar och incidenter i IT-utrustningen till alla berörda internt som externt.
- Kommunens IT ska ha sådan kontinuitetsförmåga som möjliggöra nöddrift av samhällsviktig verksamhet i alla lägen. Åtgärder ska ske samordnat med externa leverantörer.
- Kontinuitetsplanering och IT-beredskap ska övas regelbundet vid behov men minst årligen för kritiska funktioner och system.

*Personlig och gemensam IT-utrustning (hård- och mjukvara)*

- Det ska finnas ett tydligt och användarvänligt introduktionsprogram som hjälper anställda och politiker i förvaltningen att hantera kommunens IT på ett säkert och effektivt sätt. Introduktionen ska vara baserat på rutiner som vägleder den enskilde politikern och anställde i hur personlig IT-utrustning får nyttjas.
- Personlig IT-utrustning ska vara personlig och spårbar samt återanvändas inom ramen för den tekniska livslängden som leverantören angett.
- För att upprätthålla IT-säkerheten ska personlig och gemensam IT-utrustning hållas uppdaterad och ska bytas ut enligt leverantörens anvisningar eller enligt rutiner som förvaltningen beslutar.
- IT-driften och underhållet av IT-utrustning ska ta hänsyn till hållbarhetsaspekter (miljö och ekonomiska) både vid inköp och användning. Det inkluderar särskilt återbruk av utrustning utan att begränsa IT-säkerheten.
- I den mån det är tillämpbart ska extern/inhyrd personal tilldelas och nyttja kommunens IT-utrustning vid arbete åt eller i kommunens IT-miljöer.

*Loggning och spårbarhet*

- Användares arbete i system som hanterar sekretess eller i system som är avgörande för kommunens verksamheter, ska spåras och loggas för incidenthantering.

*Kryptering och behörighetsstyrning*

- Digital kommunikation ska skyddas mot obehörig insyn när det rör datatrafik till och från samt inom Hjo kommun. Särskilt ska skyddet beakta tredje parts spårning av datatrafik vid hemarbete på privata nätverk.
- Digital kommunikation som omfattas av sekretess enligt Offentlighets- och sekretesslagen och/eller dataskyddsförordningen ska skyddas från obehörig insyn genom IT-säkerhetsåtgärder.

- Meddelandefunktioner eller motsvarande funktioner inom system som hanterar sekretess eller personuppgifter ska vara skyddade mot obehörig insyn inom och utifrån systemet.

*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.
- Kopplat till rapporteringen ska förvaltningen ha en planerad och övad incidenthanteringsprocess och organisation.

*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.
- 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*

I början på varje år ska förvaltningen följa upp IT-arbetet, IT-säkerheten och systemförvaltningen 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. Se nedan.

### *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 område*, 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; personalkostnader (arbetstid) för arbetet (investeringar och åtgärder), incidenthantering och kostnader som inte varit budgeterat. Dessa ska vara förklarade och motiverade under denna rubrik.
  Sådant som varit budgeterat ska redovisas mot den faktiska kostnaden.

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 verkställts 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 inom IT.*
- *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.