



Beslutad av: Kommunfullmäktige
Framtagen av: Informationssäkerhetssamordnare
Uppdaterad:

Beslutsdatum: 2025-12-08 § 166
Dokumentansvarig: Säkerhetschef
Diarienummer: KS 2025-732
Giltighetstid: Tills vidare

Innehåll

1	Syfte	3
2	Omfattning.....	3
3	Viljeriktning	3
4	Organisation och ansvar.....	4
5	Rapportering och efterlevnad	4

1 Syfte

Denna policy utgör Osby kommuns viljeinriktning för att hantera och skydda information på ett systematiskt och informationssäkert sätt.

Informationssäkerhetspolicyn är det övergripande styrdokumentet för Osby kommuns informationssäkerhetsarbete och omfattar skydd av organisationens samlade information (kunskap och tillgångar), oavsett form, medium, lagringsplats och/eller hur informationen hanteras.

Syftet med denna policy är att skydda organisationens informationstillgångar mot obehörig åtkomst, förändring, förlust eller otillgänglighet. Policyn säkerställer att verksamheten uppfyller krav i lagstiftning, föreskrifter, avtal och interna styrande dokument.

2 Omfattning

Policyn gäller för:

- Alla kommunens verksamheter och bolag där kommunen har ett rättsligt bestämmande inflytande.
- Alla anställda, förtroendevalda, konsulter, samarbetspartners och leverantörer som hanterar organisationens information.

3 Viljeriktning

Organisationens viljeriktning är:

- Att ledningen ska ta ansvar för informationssäkerheten.
- Att uppfylla krav från tillämpliga lagar, förordningar, avtal och andra regulatoriska krav som rör informationssäkerhet.
- Att skydda informationens konfidentialitet, riktighet och tillgänglighet
- Att säkerställa att informationssäkerhet integreras i verksamhetens processer.
- Att säkerställa att informationssäkerhetsarbetet regelbundet följs upp, utvärderas och förbättras.
- Att säkerställa spårbarhet: Det ska gå att spåra vem som gjort vad, när och hur.
- Att informationssäkerhetsarbetet ska vara anpassad och proportionerlig till informationens skyddsvärde.
- Att personal ska ha kunskap om gällande informationssäkerhetsregler.
- Att säkerställa att leverantörer och samarbetspartners följer organisationens informationssäkerhetskrav under hela avtalstiden, från upphandling tills avtalsslut.
- Att tillräckliga resurser avsätts för att upprätthålla och utveckla informationssäkerhetsarbetet.
- Att definiera och utse roller inom informationssäkerhetsarbetet.
- Att säkerställa förmåga att upptäcka, hantera och återhämta sig från informationssäkerhetsincidenter och driftavbrott.
- Att säkerställa att denna viljeinriktning kommuniceras, förstås och tillämpas av alla medarbetare och relevanta parter.

Viljeriktningen ska brytas ner i en årlig handlingsplan med tillhörande prioriterade aktiviteter som ska antas i kommunledningsgruppen.

4 Organisation och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunens ledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten i den.

- **Kommunfullmäktige** uttrycker sin viljeinriktning i denna policy.
- **Kommunstyrelsen** har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- **Kommundirektören** eller **förvaltningschefen** utser systemägare och informationsägare.
- **Närmsta chef** ansvarar för att det finns rutiner och säkerställer en god efterlevnad av kommunens regelverk för informationssäkerhet.
- **Informationssäkerhetssamordnaren** har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.
- **Informationsägaren** har det övergripande och yttersta ansvaret för informationen. Informationsägarna avgör vilken information som får hanteras, hur den hanteras och av vem.
- **Systemägaren** har övergripande ansvar för ett eller flera system och dess användning. Systemen ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav. Systemens informationsmängder ska klassificeras.
- **Systemförvaltaren** är den som aktivt förvaltar systemet på systemägarens uppdrag och har helhetsansvaret samt ser till att systemets funktionalitet upprätthålls och att planerade och beslutade aktiviteter genomförs i det dagliga arbetet.
- **Dataskyddsombud** enligt Dataskyddsförordningen. Varje personuppgiftsansvarig har skyldighet att tillsätta ett dataskyddsombud med sakkunskap om lagstiftning och praxis om dataskydd. Rollen skall vara självständig, rådgivande och övervakande i att kommunen följer reglerna i Dataskyddsförordningen. Kommunen har anlitat Sydarkivera som dataskyddsombud på en kommunövergripande nivå.
- **Alla som hanterar informationstillgångar** har ett ansvar att upprätthålla och efterleva krav för informationssäkerhet.

5 Rapportering och efterlevnad

Efterlevnaden av informationssäkerhetspolicy och ledningssystemet för informationssäkerhet ska följas upp regelbundet för att säkerställa ledningssystemets fortsatta lämplighet, tillräcklighet och verkan. Informationssäkerhetssamordnaren ska årligen rapportera läge och status gällande informationssäkerhet till kommundirektören, dess ledningsgrupp och kommunstyrelsen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.