ORSA KOMMUN

POLICY FÖR INFORMATIONSSÄKERHET OCH DATASKYDD

Alla verksamheter och bolag inom Mora, Orsa och Älvdalens kommuner ska på alla nivåer bedriva ett aktivt och systematiskt informationssäkerhetsarbete så att rätt information finns tillgänglig för rätt personer vid rätt tidpunkt. Informationstillgångar ska inte hamna i orätta händer och missbrukas.

ORSA KOMMUN

Innehållsförteckning

ORSA KOMMUN

1. Policyns roll

Policyn är ett centralt styrdokument som redovisar kommunerna och dess bolags viljeinriktning och mål inom informationssäkerhet och dataskydd.

Policyn styr informationssäkerhetsarbetet och kompletteras med särskilda instruktioner, rutiner och regler som ger verksamheterna förutsättningar och stöd i informationssäkerhetsarbetet.

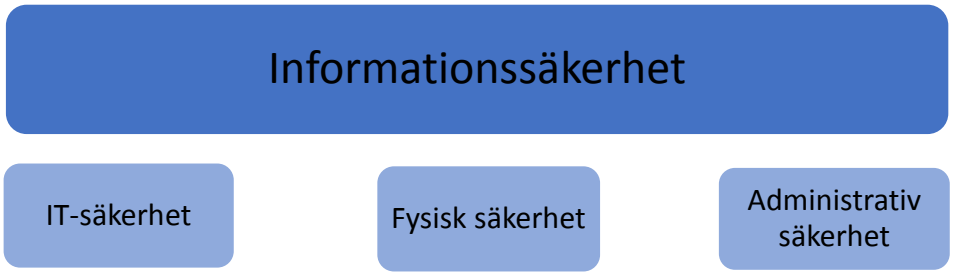
Alla verksamheter omfattas av policyn, vilket medför att det inte finns utrymme för lokala avvikelser. Policyn utgör grunden för det systematiska arbetet med informationssäkerhet och ska även tillgodose de krav på informationssäkerhet som ingår i dataskyddsförordningen.

2. Inledning

Kommunerna och dess bolag hanterar stora mängder information. Det är viktigt att medborgare, företag och organisationer har fortsatt tillit och förtroende för att vi hanterar både analog och digital information korrekt och att den skyddas. Säkerheten för informationen är därför mycket viktig för alla våra verksamheter och även en förutsättning för att kunna vara en del av samhällsutvecklingen och att lyckas med digitalisering.

Informationssäkerhet kan delas upp i:

- IT-säkerhet - skydd för digital information när man behandlar, överför och lagrar den.
- Fysisk säkerhet – åtkomst till informationstillgångar, intrångsdetektering, larm, behörighetskontrollsystem, skalskydd.
- Administrativ säkerhet - riktlinjer, styrning, organisation, regler och rutiner.



I maj 2018 kom uppdaterad dataskyddslagstiftning som styr hur vi får behandla information innehållande personuppgifter, och även här ställs informationssäkerhetskrav.

Brister i informationssäkerhet kan leda till risk för liv och hälsa, hot mot den personliga integriteten samt leda till negativ ekonomisk påverkan och att förtroendet för kommunerna skadas.

Sammantaget har vi stora krav på informationssäkerhet och därför är systematik och en fast styrning nödvändig för att upprätthålla säkerhet och kvalitet. Informationssäkerhetsarbetet ska vara en del av kommunens övriga lednings- och kvalitetsprocess.

ORSA KOMMUN

3. Målsättning

Vi ska utöva ett systematiskt informationssäkerhetsarbete för att nå övergripande visioner, strategier och mål.

För vårt informationssäkerhetsarbete gäller att:

- informationssäkerhetskulturen ska verka engagerande och motivera till att ständigt förbättra informationssäkerheten
- all personal har kunskap om gällande informationssäkerhetsregler
- vi ska efterleva krav i lagar, förordningar, föreskrifter och avtal
- vi får rätt nivå av skydd vad gäller tillgänglighet, riktighet, konfidentialitet och spårbarhet utifrån en fastställd organisationsgemensam modell för informationsklassning
- hotbilden mot informationstillgångarna analyseras fortlöpande med hjälp av risk- och sårbarhetsanalyser
- vi bedriver ett förebyggande arbete så att händelser som kan leda till negativa följder undviks
- vi har incidenthanteringsplaner
- medborgares och externa verksamheters förväntningar och behov kan mötas.

4. Principer och arbetssätt

Vi ska arbeta efter den etablerade standardserien SS-ISO/IEC 27000 för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för informationssäkerhet (LIS).

Vi ska ha årliga mål för informationssäkerhetsarbetet i verksamhetsplaneringen. I målen ska anges:

- vad som ska göras under året och hur,
- när och hur medarbetarna ska informeras och utbildas,
- när och hur uppföljning och utvärdering ska ske samt avrapportering,
- behov av ekonomiska och personella resurser.

5. Roller och ansvar

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret.

Den politiska ledningen i form av kommunfullmäktige, kommunstyrelse, nämnder och bolagsstyrelser har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom deras ansvarsområden och ska ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och besluta om åtgärder.

Verksamhetsansvariga ansvarar för information inom sin verksamhet och dess säkerhet. Säkerställer att det finns rätt kompetens i organisationen. Ansvarar för att medarbetarna har ett säkerhetsmedvetande och tillräcklig kunskap för att informationssäkerhet kan uppnås.

Medarbetare ansvarar för att följa policy för informationssäkerhet, riktlinjer, rutiner och regler. Man ansvarar även för att vara uppmärksam på brister och incidenter rörande informationssäkerhet.

Informationssäkerhetssamordnaren har det övergripande ansvaret att leda och samordna informationssäkerhetsarbetet och arbetar i samråd med utsedda inom administrativ säkerhet, fysisk säkerhet och IT-säkerhet, dataskyddsombud samt verksamhetsrepresentanter.

Dataskyddsombudet har en stödjande, vägledande roll i organisationen och ska tillse efterlevnad av gällande dataskyddslagstiftning. Kontaktperson för de registrerade, för den egna organisationen och för tillsynsmyndigheten.

ORSA KOMMUN

6. Uppföljning

Uppföljning i verksamheterna är en viktig del av det systematiska informationssäkerhetsarbetet och ska utföras för att bevaka att:

- beslutade åtgärder är genomförda,
- årliga mål är uppfyllda,
- regler följs,
- säkerhetsinstruktioner och riskanalyser hålls uppdaterade.

Informationssäkerhetssamordnaren ska kontrollera och följa upp informationssäkerheten internt och rapportera till kommundirektör, samt ansvara för att Informationssäkerhetspolicyn ses över årligen.

Dataskyddsombudet ska genom fortlöpande kontroller säkerställa att gällande dataskyddslagstiftning efterföljs och om så inte sker, rapportera till personuppgiftsansvarig, kommundirektör samt i vissa fall till tillsynsmyndigheten.

7. Begrepp

Begrepp	Definition
Informationstillgångar	Allt som innehåller information och allt som bär på information.
Dataskydd	Den lagstiftning som reglerar behandling av personuppgifter. Integritetsskydd.
Informationssäkerhet	De åtgärder som vidtas för att säkerställa konfidentialitet, riktighet och tillgänglighet. Det omfattar administrativ säkerhet, fysisk säkerhet och IT-säkerhet.
Konfidentialitet	Att informationstillgångar inte kan nås av obehöriga.
Riktighet	Att informationstillgångar skyddas från oönskad förändring eller radering.
Tillgänglighet	Att informationstillgångar är tillgängliga inom önskad tidsrymd.
Spårbarhet	Att vi kan spåra vem som har gjort vad med informationen.
LIS	Ett strukturerat sätt att arbeta med informationssäkerhet som bygger på den svenska och internationella standarden för LIS, som hjälper oss att hålla önskad nivå av informationssäkerhet i organisationen.