Mörbylånga kommun

POLICY

Datum
2018-07-23

Dnr
2018/000703-005

Dokumentansvarig
Jonas Jansson, 0485-471 25
jonas.jansson@morbylanga.se

Beslutande
Kommunfullmäktige
2017-02-28

Beteckning

Reviderad
2018-08-28

Handbok

Giltighetstid
2018-09-01

Aktualitetsprövning/revidering senast
2019

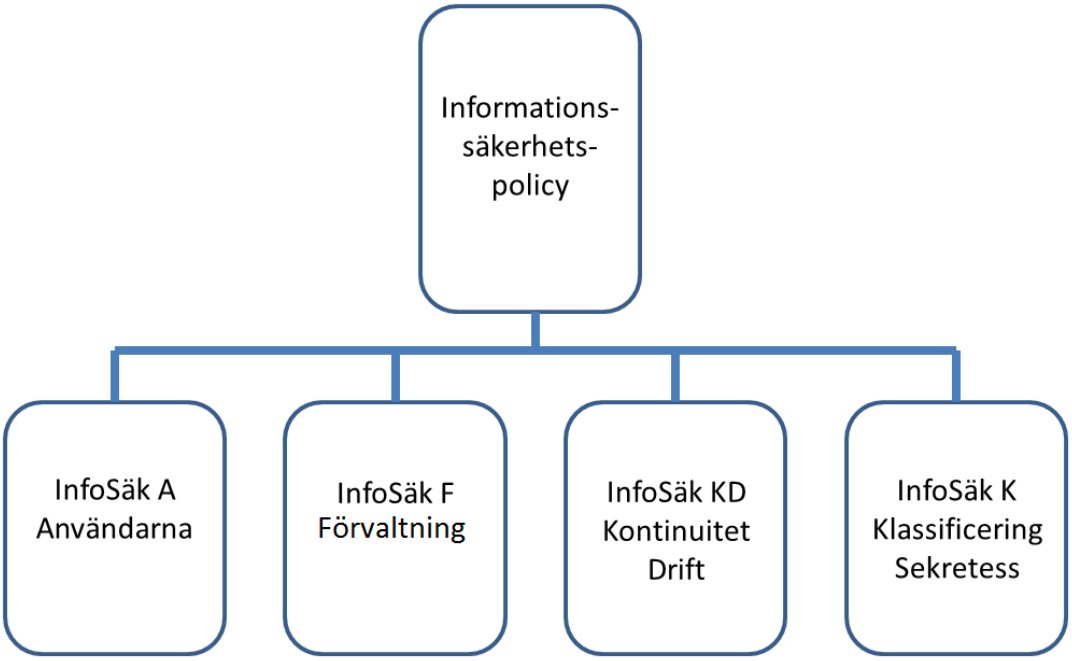
Dokumentkategori

- ○ Författningssamling
- ◉ Övergripande styrdokument
- ○ Verksamhetseget dokument

Dokumentkoppling

Informationssäkerhetspolicy

Innehåll



Bilden visar strukturen för kommunens informationssäkerhetspolicy. Policyn med bilagona InfoSäk A, F, KD och K, hänvisar i sin tur till dokument som i detalj styr kommunens arbete med utgångspunkt i dataskyddsförordningen och Lag (2018:218) med kompletterande bestämmelser till EU:s dataskydds-förordning, här fortsättningsvis benämnd dataskyddslagen. Bilagorna utgör riktlinjer för detta policydokument.

Vad är en informationssäkerhetspolicy?

Informationssäkerhetspolicyn med sina bilagor är det övergripande dokument som anger mål och inriktning, samt styr verksamhetens arbete med informationssäkerhet.
Informationssäkerhetspolicyn utgör verksamhetens gemensamma plattform för detta arbete.
I detta policydokument används begreppet ”informationssystem” istället för ”verksamhetsystem”.

Vad är informationssäkerhet?

Information kan förekomma i många former: den kan tryckas eller skrivas på papper, lagras elektroniskt, överföras med post eller med elektroniska hjälpmedel, visas på film eller yttras i en konversation. Informationen kan dock behöva ett godtagbart skydd oavsett vilken form den antar, eller hur den överförs eller lagras.
Ett informationssäkerhetsarbete är således arbetet med att uppnå önskad nivå av *riktig*, *tillgänglig*, *spårbar* samt *sekretesskyddad* (konfidentiell) information.
Informationssäkerhet är en integrerad del av en kommuns verksamhet. Alla som hanterar informationstillgångar har ett ansvar för att upprätthålla informationssäkerheten. Chefer på alla nivåer har dessutom ett ansvar i att aktivt verka för en positiv attityd till informationssäkerhetsarbetet. Alla verksamheter är skyldiga att systematiskt arbeta med informationssäkerhet.

Det ska vara en naturlig del i arbetet och ska ingå som en stående punkt vid arbetsplatsträffar och på chefsmöten.
Alla incidenter som påverkar kommunens informationssäkerhet ska skyndsamt rapporteras.

- Påverkar incidenten en programvara så att en funktion plötsligt slutar att fungera ska den rapporteras till systemförvaltaren. Blankett för incidentrapportering finns på kommunens intranät.
- Påverkar incidenten hårdvaran (exempel dator, skrivare, nätverk) ska den rapporteras till IT-avdelningens helpdesk.
- Gäller det en personuppgiftsincident ska den rapporteras till informationsägaren (närmast ansvarig chef). I dataskyddsförordningen definieras begreppet personuppgiftsincident som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna betraktas också som en personuppgiftsincident.. Blankett för incidentrapportering finns på kommunens intranät.

Alla verksamheter inom kommunen omfattas av informationssäkerhets-policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som ger en lägre säkerhetsnivå.
Den som använder kommunens informationstillgångar på ett sätt som strider mot denna policy och tillhörande riktlinjer kan bli föremål för arbetsrättsliga åtgärder.

Vad omfattas

Informationssäkerheten omfattar kommunens alla informationstillgångar.
Exempel på informationstillgångar är:

- Information som finns i datorer eller på servrar,
- information som skickas med e-post, chatt eller liknande,
- information som finns på mobila enheter till exempel telefoner och surfplattor,
- information som finns lagrad på externt media ex USB-minne med mera.
- information som visas på webbsidor eller via sociala medier,
- information som överförs muntligt via ett samtal med telefon, direkt eller annat media,
- information som finns i skriftlig form (se även gällande dokument-hanteringsplaner).

De centrala begreppen

Begreppen *konfidentialitet* (sekretesskyddad), *riktighet*, *tillgänglighet* och *spårbarhet* är centrala i arbetet för att nå god informationssäkerhet.

- Konfidentialitet - att obehöriga inte får ta del av uppgifterna.
- Riktighet - att informationen ska vara tillförlitlig, korrekt och fullständig.
- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.
- Spårbarhet - att aktiviteter som rör informationen kan spåras.

Mål för kommunens informationssäkerhetsarbete

För att du ska få den information som du behöver, vid rätt tidpunkt och med korrekt innehåll, är de övergripande målen för informationssäkerhetsarbetet att vi ska:

- Behandla information på ett tydligt, korrekt, säkert och relevant sätt.
- Kunna leverera och hämta information vid rätt tidpunkt.

I bilagorna InfoSäk A, F, KD och K, finns mer detaljerade anvisningar för hur vi ska arbeta för att uppnå målen.

Kommunens övriga mål med informationssäkerhetsarbetet är att:

- All personal har tillräcklig kunskap om gällande informationssäkerhetsregler (se även dokumentet InfoSäk A).
- Alla tillgångar både i form av information samt teknisk utrustning har skydd i tillräcklig grad.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation.
- Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten analyseras regelbundet (se även dokumentet InfoSäk F).

Roller och ansvar

Personuppgiftsansvarig
Kommunfullmäktige och de olika nämnderna är personuppgiftsansvariga, var och en i sin verksamhet. Den personuppgiftsansvarige har ansvar för att behandlingen av personuppgifter sker på ett lagligt och korrekt sätt i enlighet med dataskyddsförordningens krav. Det innebär bland annat att man ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgiftsbehandlingen sker på ett integritetsrättsligt säkert sätt.

Personuppgiftsbiträde
Personuppgiftsbiträdet är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

Dataskyddsombud
Dataskyddsombudet informerar och ger råd, övervakar behandlingen av personuppgifter samt påpekar vid behov fel och brister till den som är personuppgiftsansvarig.

Dataskyddssamordnare
Dataskyddssamordnaren är den person i kommunen som har det samordnande ansvaret för integritetsskyddsfrågor inom gällande dataskyddslagstiftning och den som bistår dataskyddsombudet i frågor som rör personuppgiftshantering.

Risk- och informationssäkerhetschef
Rådgivande funktion med placering på Ölands räddningstjänst i Ölands kommunalförbund. Funktionen ger stöd till Ölandskommunerna i arbetet med bland annat informationssäkerhet.

Förvaltningschef
Ansvarar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige fastställda informationssäkerhetspolicyn. Förvaltningschefen ansvarar för att systemägare utses för respektive informationssystem. Så länge annan systemägare inte är utsedd är förvaltningschefen systemägare.

Systemägare
Har det ekonomiska ansvaret och är ansvarig för säkerheten i sitt system i alla frågor som rör informationssäkerhet och ansvarar också för att behandlingen är laglig.

Systemförvaltare
Den som aktivt förvaltar IT-systemet på systemägarens uppdrag. Systemförvaltaren biträder systemägaren i alla frågor som rör informationssäkerhet.

Informationsägare
Närmast ansvarig chef som äger informationen och ansvarar för att den är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren ansvarar för att informationssäkerheten hålls på en hög nivå.

IT-chef
Leder IT-avdelningens arbete med driftsäkerhet och även att denna överensstämmer med systemägarens anvisningar. IT-chefen bygger upp nödvändiga nätverk och svarar för att IT-avdelningen har en uppdaterad förteckning över kommunen samtliga IT-system.

Användare
Den som använder kommunens informationssystem i det dagliga arbetet.

Revidering och uppföljning

Uppföljning är en viktig del av informationssäkerhetsarbetet och ansvaret att så sker ligger på systemägaren och informationsägaren (närmast ansvarig chef). Uppföljningen ska bevaka:

- Att beslutade åtgärder är genomförda.
- Att mål är uppfyllda.
- Att riktlinjer följs.

Uppföljningen ska årligen rapporteras in till kommundirektören som sammanställer en rapport till nämnderna. Rapporten som ska vara

färdigställd vid halvårskiftet och avse föregående kalenderår ska också lämnas till dataskyddssamordnaren för kännedom.

Policy och riktlinjer

Kommundirektören ansvarar för att denna policy med bilagor löpande följas upp och revideras vid behov. Bilagorna InfoSäk A, F, KD samt K, fastställs av kommunstyrelsen att gälla för samtliga nämnder.

Särskilda rutiner

Vissa områden inom ämnet informationssäkerhet är av särskild betydelse för organisationens verksamhet.
Av informationssäkerhetsinstruktionerna nedan ska områden och de särskilda riktlinjer, regler och rutiner som gäller för dessa, framgå enligt följande:

InfoSäk A (Användare)

Vänder sig till användarna. Tar bland annat upp områdena behörighet, inloggning och lösenord, utrustning, upplåtelse av arbetsplats, programvaror, hantering av information, utskrifter, e-post, virus, distansarbete, IT-incidenthantering och användning av Internet.

InfoSäk F (Förvaltning)

Roller och ansvar. Tar bland annat upp områdena behörighetsadministration, behörighetskontroll, loggning och spårbarhet, risk- och sårbarhetsanalys, införande, driftgodkännande, avveckling av informationssystem.

InfoSäk KD (Kontinuitet och Drift)

Informationssäkerhetsinstruktion Kontinuitet och drift gäller för kommunens IT-organisation (IT-avdelningen). Tar bland annat upp områdena helpdesk, säkerhet, krav på nätverk, system- och driftdokumentationer, förvaring.

InfoSäk K (Klassificering)

Tar upp klassificering och sekretess.