Falkenbergs kommun

Riktlinje – styrning av informationssäkerhet

Diarienummer	Fastställt av	Datum för fastställande
2023/370	Kommunstyrelsen	
Dokumenttyp	Dokumentet gäller för	Giltighetstid
Riktlinje	Samtliga nämnder och helägda bolag	Tills vidare
Revideringsansvarig	Revideringsintervall	Reviderad datum
Kommunstyrelsen	Vart fjärde år	2023-12-05
Dokumentansvarig (funktion)	Uppföljningsansvarig och tidplan (se punkt 5)	
Infosäksamordnare	Respektive nämnd och bolag	

Falkenbergs kommun
31180 Falkenberg. Telefon växel: 0346-88 60 00.
e-post: kontaktcenter@falkenberg.se
kommun.falkenberg.se

1. Syfte

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för information utifrån dess skyddsvärde. Kommunens information ska inte avslöjas eller vara tillgänglig för obehöriga. Målet är att rätt information ska vara tillgänglig för rätt person vid rätt tillfälle.

Kommunens informationssäkerhetsarbete ska bidra till att Falkenbergs kommun är trygg och säker för alla som bor, vistas och verkar i kommunen.

Syftet med denna riktlinje är att ange hur det systematiska informationssäkerhetsarbetet ska bedrivas i Falkenbergs kommun och hur ansvarsfördelningen för arbetet ser ut.

Riktlinjen riktar sig i första hand till dem som arbetar med IT- och informationssäkerhet eller har ansvar för informationssäkerhet i förvaltningsobjekt, projekt, processer eller andra verksamheter.

2. Riktlinje

Informationssäkerhetsarbetet i Falkenbergs kommun ska vara riskbaserat, systematiskt och utgå från Myndigheten för samhällsskydd och beredskaps metodstöd.

2.1 Hantering av informationstillgångar

Organisationens informationstillgångar ska identifieras och informationsägare ska utses för varje tillgång. Informationsägaren ansvarar för att informationsklassning och riskanalyser genomförs. De ansvarar vidare för att informationen hanteras på ett ändamålsenligt sätt utifrån de krav informationsklassningen anger.

Informationsklassning ska vara en central aktivitet i informationssäkerhetsarbetet och syftar till att bedöma informationens värde för kommunens verksamhet samt säkerställa lämpligt skydd utifrån skyddsvärdet. Bedömning sker såväl utifrån den egna verksamhetens behov som utifrån externa krav. Allmänt accepterad metod ska användas för informationsklassning. Säkerhetsavdelningen bistår med metod för klassning och stöd i arbetet.

Hantering av information i verksamhetssystem och digitala verktyg ska följa Falkenbergs kommuns systemförvaltarmodell.

2.2 Riskanalys

Informationssäkerhetsarbetet ska utgå från riskanalyser som syftar till att ange rätt skyddsnivå i alla delar av verksamheten för att:

• förhindra eller försvåra för obehöriga att få tillgång till information
• säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig
• bidra till att informationen är åtkomlig för behörig person vid rätt tillfälle.

Riskanalys utifrån informationssäkerhet ska genomföras inför upphandling av förvaltningsgemensamma IT-stöd. Säkerhetsavdelningen bistår med metodstöd och mallar. Riskägaren, ofta informationsägaren, beslutar om hur riskerna ska hanteras utifrån riskanalysen.

Genomförda riskanalyser ska följas upp av riskägaren för att kontrollera kvarvarande risker med hänsyn till förändringar i verksamhet, skyddsåtgärder, hotbild och lagkrav.

Särskilda krav gäller för riskanalys i samband med behandling av personuppgifter.

2.3 Kontinuitetshantering för informationstillgångar

En god kontinuitetshantering säkerställer att kritisk verksamhet kan bedrivas på en acceptabel nivå oavsett störningar som påverkar tillgången till information.

Kontinuitetsplaner för att säkerställa tillgång till kritisk information ska finnas för varje samhällsviktig verksamhet samt för stödfunktioner, Planerna ska finnas tillgängliga för behöriga medarbetare och förvaras och hanteras utifrån informationsägarens anvisningar.

2.4 Incidenthantering

En incident definieras som en oönskad händelse med negativa konsekvenser. För anmälan av incidenter/misstänkta incidenter ska det finnas rutiner och särskilda kanaler. Säkerhetsavdelningen ansvarar för framtagande av rutiner och bistår med stöd.

Rapporterade incidenter hanteras i kommande riskanalyser.

2.5 Anskaffning, utveckling och underhåll av system

Respektive verksamhet ansvarar för att vid anskaffning, utveckling och avveckling av externa IT-tjänster, som till exempel datasystem och molntjänster, säkerställa rätt nivå av Informationssäkerhet utifrån informationens skyddsvärde.

För att uppnå rätt nivå av informationssäkerhet för IT-tjänster krävs:

• Att informationsklassificering med tillhörande riskanalys genomförs och resultatet ligger till grund för informationssäkerhetskrav vid upphandling. För vissa personuppgiftsbehandlingar krävs därutöver en särskild risk- och konsekvensbedömning utifrån dataskyddsförordningen.
• Servicenivåavtal (SLA) med leverantören.

2.6 Ledningens genomgång

Informationssäkerhetssamordnaren ska årligen rapportera informationssäkerhetsarbetets läge och status till koncernledningsgruppen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

Respektive förvaltning och bolag bidrar med underlag utifrån sin verksamhet till informationssäkerhetssamordaren inför ledningens genomgång.

3. Definitioner och avgränsningar

Riktlinjerna gäller för alla kommunala verksamheter och helägda bolag och omfattar alla informationstillgångar som kommunen hanterar.

Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild inkluderas.

4. Ansvar och uppföljning

Kommunstyrelsen ansvarar för att leda, samordna och utveckla kommunens strategiska informationssäkerhetsarbete.

Varje nämnd och bolagsstyrelse är ytterst ansvarig för informationssäkerheten, inklusive personuppgiftsansvarig, inom sitt verksamhetsområde. Vid behov kan varje nämnd och styrelse besluta om mer detaljerade anvisningar inom ramen för denna riktlinje.

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Informationssäkerhetssamordnaren och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd i arbetet. Dataskyddsombudet och övriga som arbetar specifikt med personuppgiftsbehandlingar, t ex personuppgiftssamordnarna, fungerar som stöd i arbetet avseende information innehållande personuppgifter. Ombudets roll är också att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen.

Varje medarbetare ansvarar för att följa gällande styrdokument för informationssäkerhet samt rapportera informationssäkerhetsrelaterade brister och incidenter.

5. Koppling till lagstiftning och andra styrdokument

EU:s NIS-direktiv har införts i Sverige genom lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen hanterar krav på säkerhet i nätverk och informationssystem och omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster inom utpekade sektorer. Utöver lagen finns förordning om informationssäkerhet för samhällsviktiga och digitala tjänster och ett antal föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB).

Genom dataskyddsförordningen och där tillhörande lagar skyddas människor mot att deras personliga integritet kränks vid behandling av personuppgifter. Förordningen innehåller också regler om vilka tekniska hjälpmedel och säkerhetsåtgärder som behöver vidtas vid hantering av personuppgifter.

MSB har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete. Metodstödet syftar till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas och användas utifrån standarderna om ledningssystem för informationssäkerhet. Kommunens informationssäkerhetsarbete följer metodstödet.

Kommunfullmäktige har antagit en säkerhetspolicy som anger inriktning och ramar för kommunens säkerhetsarbete. Därtill finns ytterligare riktlinjer och anvisningar inom informationssäkerhetsområdet.