STYRDOKUMENT

Riktlinje för Informationssäkerhet

Beslutad när	2021-06-23 §110
Beslutad av	Kommunfullmäktige
Diarienummer	KSKF/2020:360
Ersätter	Informationssäkerhetsplan KSKF/2014:112
Gäller för	Samtliga nämnder och bolag
Gäller fr o m	2021-06-23
Gäller t o m	Tillsvidare
Dokumentansvarig	Kommundirektör
Uppföljning	Årlig rapport KS

Program
Ett program är ett styrande dokument som ska visa en färdriktning genom att innehålla vad som ska uppnås inom ett visst område. Det tar inte ställning till utförande, prioriteringar och metoder. Program ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Plan
En plan är ett styrande dokument som ska visa en färdriktning genom att innehålla konkreta mål och riktlinjer. Den ska vara tidsbegränsad och beslutas av kommunfullmäktige.

Policy
En policy är ett styrande dokument som ska visa ett övergripande förhållningssätt och som ska tjäna som vägledning inom ett område, med angivande av övergripande mål och värden som ska eftersträvas. Policys ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Riktlinje
En riktlinje är ett styrande dokument som ska säkerställa ett korrekt agerande och god kvalitet i handläggning och utförande. Riktlinjer ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Ämnesområde och bakgrund

Denna riktlinje anger Eskilstuna kommunkoncerns (Kommunkoncernen) inriktning och övergripande principer för informationssäkerhet, liksom roller och definitioner inom området. Kommunkoncernens alla verksamheter omfattas av riktlinjen.

Denna riktlinje och tillhörande anvisningar och rutinbeskrivningar ersätter tidigare informationssäkerhetsplan (KSKF 2014:112) och tillhörande användarinstruktioner.

Bolagen har utifrån de specifika krav som riktas mot dess verksamhet, möjlighet att ge ut bolagsanpassade styrdokument.

Om informationssäkerhet

Information finns i Kommunkoncerns alla verksamheter och handlar om allt det vi gör, därav är informationen en av Kommunkoncernens viktigaste tillgångar.

Informationssäkerhet omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan t.ex. vara i form av text, ljud, bilder och film och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Grundförutsättningen för att Kommunkoncernen ska kunna utföra sitt uppdrag gentemot invånare, brukare, medarbetare och elever är att all informationshantering behöver hanteras utifrån principen: rätt information, vid rätt tillfälle, till rätt person

Information som kommer obehöriga till del, är felaktig, manipulerad eller som inte är tillgänglig när den behövs, kan orsaka skada för den enskilde, ökade kostnader samt påverka samhällets förtroende för Kommunkoncernen. Arbete med informationssäkerhet ska alltid vara riskbaserat, med medvetenhet om vilken skada som kan åsamkas Kommunkoncernens invånare, brukare, medarbetare, elever och verksamhet.

För att nå ovanstående princip behöver informationen hanteras utifrån:

- Konfidentialitet: åtkomst endast för behöriga
- Riktighet: korrekt och inte felaktigt förändrat av misstag eller avsiktligt
- Tillgänglighet: åtkomlig och kan nyttjas inom önskad tid

De skydd vi har att tillgå för att skydda informationen är av karaktär:

- Digitala/Tekniska skydd: skydd via IT-komponenter, tex behörighetssystem, brandväggar, antivirusprogram, flerfaktors autentisering, kryptering
- Fysiska skydd: t.ex. skal- och brandskydd i lokaler, låsbara skåp, larm, kameror
- Administrativa skydd: styrande och stödjande dokument
- Mänskliga skydd: kunskap om hur informationen får hanteras och kommuniceras, kan t.ex. förmedlas via utbildning, information samt processer och metoder.

En kombination av flera skyddsåtgärder bör användas för att skapa flera barriärer.

Mål med informationssäkerhet

Informationssäkerhet har inget egenvärde. Arbetet ska bidra till att Kommunkoncernen når sina övergripande visioner, strategier och mål. Kommunkoncernen ska uppnå och upprätthålla en informationssäkerhet som

- innebär en robust, säker och tillförlitlig informationshantering
- möjliggör ett aktivt medverkande i det digitala samhället
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet
- motsvarar medborgares och externa verksamheters behov och förväntningar
- uttrycks i aktuella styrdokument som riktlinje och anvisningar
- efterlever krav i lagar, förordningar, föreskrifter och avtal

Principer och arbetssätt

Kommunkoncernen behöver arbeta med informationssäkerhet så att ovanstående mål uppfylls. Styrande dokument avseende informationssäkerhet ska gentemot Kommunkoncernens verksamheter vara normerande och stödjande, beskriva arbetssätt för efterlevnad, kontroll och uppföljning. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Kommunkoncernens informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Kommunkoncernen ska

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik
- vara systematisk och bygga på den etablerade standardserien SS-ISO/IEC 27000[1].
- löpande ses över och förbättras, eftersom Kommunkoncernen och dess omvärld, inklusive hotbild, är under ständig förändring

[1] Enligt tidigare fattat beslut är certifiering inget krav inom kommunen.

- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa
- vara i samklang med Kommunkoncernens mål och vision och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild
- vara väl kommunicerad till verksamheten. Alla medarbetare ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande samt för att kunna leva upp till denna riktlinje och underliggande anvisningar för informationssäkerhet
- ske i aktiv samverkan med Kommunkoncernen och externa intressenter, såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet som t.ex. SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap), IMY (Integritetsskyddsmyndigheten) och SIS (Swedish Standards Institute).

Roller och ansvar

Kommunfullmäktige/Bolagsstyrelse. Kommunfullmäktige fastställer koncernövergripande policyer, riktlinjer och planer. Bolagsstyrelse beslutar om eventuellt anpassad policy, riktlinjer etc för den egna verksamheten.

Nämnd/Koncernledning fattar beslut i frågor som är avgränsade till den egna förvaltningen/bolaget och är ytterst ansvarig för att riktlinjen tillämpas i den egna verksamheten.

Kommundirektör/VD. Kommundirektör beslutar i frågor som har betydande påverkan på kommunens verksamhet och ekonomi, efter förankring i koncernledningsgruppen. Fastställer kommungemensamma anvisningar. VD beslutar i frågor som har betydande påverkan på bolagens verksamhet och ekonomi.

Kommunledningskontoret, Kommunstrateg informationssäkerhet är ansvarig att förvalta styrande dokument inom området informationssäkerhet. I detta ingår att förvalta, revidera och följa upp efterlevnad av de styrande dokumenten på en övergripande nivå.

Verksamhetsansvariga (chefer) är ansvariga för att riktlinje och anvisningar för informationssäkerhet tillämpas och efterlevs inom respektive verksamhet bland annat att medarbetare har förutsättningar att hantera Kommunkoncernens information på ett säkert sätt enligt gällande regler, att informationssäkerhetsincidenter rapporteras och att anskaffning sker enligt rådande beslut.

Processägare och Objektägare följer upp att riktlinje och anvisningar inom område informationssäkerhet efterlevs inom respektive process och objektet. Process- och objektägare ska regelbundet rapportera aktuell status för området till verksamhetsansvarig.

Medarbetare är skyldiga att behandla Kommunkoncernens information i enlighet med gällande riktlinje och anvisningar.

Serviceförvaltningen/IT-avdelningen inom bolagen ansvarar för implementation av delar som berör IT-enheternas ansvar samt bevakar efterlevnad av riktlinje och anvisningar i den löpande driften. Avsteg från efterlevnad följs upp för åtgärd.

Uppföljning och rapportering

Efterlevnaden av informationssäkerhetsriktlinjen och anvisningar för informationssäkerhet ska följas upp regelbundet.

Kommunstrateg informationssäkerhet ska årligen rapportera läge och status gällande informationssäkerhet till kommundirektören och kommunstyrelsen. Säkerhetsfunktionen inom respektive bolag ska på samma sätt årligen rapportera läge och status gällande informationssäkerhet till VD respektive bolagsstyrelse.

Rapportering till tillsynsmyndigheter ska ske utifrån respektive organisations rapporteringsskyldighet.

Särskilda skäl som till exempel allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

Förhållande till redan fattade politiska beslut och lagstiftning

Riktlinje för informationssäkerhet kompletteras med Anvisningar för informationssäkerhet. Dessutom relaterar riktlinjen till IT-policy (KSKF/2020:187), IT-plan (KSKF/2020:188), Eskilstunas program för digital transformation (KSKF 2019:351) samt riktlinjer inom IT-området.

Lagar och förordningar ställer krav på kommuners informationssäkerhet. Följande lagar och förordningar ställer direkt eller indirekt krav på informationssäkerheten (med reservation för att andra lagar och förordningar också kan ha påverkan på informationshanteringen):

- *Dataskyddsförordningen (Europaparlamentets och rådets förordning 2016/679)*
- *Dataskyddslagen (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning)*
- *Tryckfrihetsförordningen (1949:105)*
- *Offentlighets- och sekretesslagen (2009:400)*
- *Säkerhetsskyddslagen (2018:585)*
- *Arkivlagen (1990:782)*
- *Lag om behandling av personuppgifter inom socialtjänsten (2001:454)*
- *Förvaltningslagen (2017:900)*
- *Patientdatalagen (2008:355)*
- *Kommunallagen (2017:725)*
- *Lag om offentlig upphandling (2016:1145)*
- *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174, sk NIS-direktivet*
- *Arbetsmiljölag (1977:1160)*