Informationssäkerhets- och dataskyddspolicy

Beslutad av kommunfullmäktige 2022-01-27.

Denna policy med tillhörande riktlinjer och instruktioner
ersätter den som beslutades av kommunfullmäktige 2010-10-07

FALUN

Innehåll

Om informationssäkerhets- och dataskyddspolicyn **3**
Syfte **3**
Mål **3**
Strategiska mål 3
Övergripande mål 3
Årliga mål 3
Aspekter och principer **4**
Informationssäkerhetsaspekter 4
Dataskyddsprinciper 4
Roller och ansvar **5**
Informationssäkerhet 5
Dataskydd 5
Verksamhetsdriven informationssäkerhet genom informationssäkerhetsklassning 5
Förutsättningar 5
Avvikelser **5**
Granskning, uppföljning och rapportering **5**
Ansvar för policyn **5**

Om informationssäkerhets- och dataskyddspolicyn

Informationssäkerhets- och dataskyddspolicyn är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Styrdokumentet *Riktlinjer för informationssäkerhet* är mer detaljerat och konkretiserar informationssäkerhets- och dataskyddspolicyn.

Informationssäkerhets- och dataskyddspolicyn gäller för informationssäkerhet och dataskydd inom Falu kommun, och kompletterar kommunens övriga styrdokument.

Alla kommunens verksamheter omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Informationssäkerhets- och dataskyddspolicyn gäller inte för kommunens bolag, undantaget när de använder sig av kommunens gemensamma informationstillgångar, eller då det finns särskilda behov av samordning.

Syfte

Information och personuppgifter är av grundläggande betydelse för kommunens verksamheter. Att information och personuppgifter hanteras enligt dess skyddsvärde har betydelse för förtroendet för Falu kommun samt för integriteten hos personer vars personuppgifter kommunen hanterar. Inom vård och omsorg kan det till och med vara livsavgörande. I enstaka fall kan också viss information vara av betydelse för Sveriges säkerhet.

Syftet med informationssäkerhets- och dataskyddspolicyn är att påvisa kommunfullmäktiges vilja att information, personuppgifter, och säkerhetsskyddsklassificerade uppgifter[1] samt verksamhetssystem, lagringsytor och kommunikationskanaler hanteras i enlighet med gällande lagar samt uppsatta mål, aspekter och principer.

Systematiskt och riskbaserat informationssäkerhetsarbete syftar till att Falu kommun långsiktigt ska säkerställa informationens konfidentialitet, riktighet och tillgänglighet, samt i vissa fall spårbarhet, baserat på dess skyddsvärde och aktuell hotbild (se Informationssäkerhetsaspekter nedan).

Systematiskt dataskyddsarbete syftar till att långsiktigt säkerställa att Falu kommun uppfyller dataskyddsprinciperna enligt artikel 5 i dataskyddsförordningen, GDPR[2] (se Dataskyddsprinciper nedan).

[1] Enligt Säkerhetsskyddslagen (2018:585), Säkerhetsskyddsförordningen (2018:658) och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2)

[2] General Data Protection Regulation, Europaparlamentets och rådets förordning (EU) 2016/679

Mål

Strategiska mål

Falu kommun ska införa och förvalta Ledningssystem för informationssäkerhet och dataskydd (LISD) enligt den internationella standardserien för informationssäkerhet, SS-ISO/IEC 27000. Med LISD skapas tydlighet och struktur samt förutsättningar för ett systematiskt arbetssätt.

Kommunens personuppgiftsbehandling ska ske i enlighet med GDPR, Dataskyddslagen (SFS 2018:218) samt övrig dataskyddslagstiftning.

Kommunen ska skapa förutsättningar för digitalisering med väl avvägd säkerhetsnivå i kommunens verksamheter.

Övergripande mål

Övergripande mål för informationssäkerhetsarbetet är att det ska

- utföras i enlighet med legala krav
- utföras i enlighet med krav i LISD
- vara väl avpassat, ändamålsenligt och kostnadseffektivt samt dimensionerat efter verksamheternas förutsättningar och behov
- möjliggöra för verksamheterna att själva ta kontroll över information och personuppgifter de hanterar
- vara dimensionerat efter behovet av säkerhetsskydd
- vara robust och säkerställa likvärdigt skydd oavsett om verksamheten drabbas av en mindre störning eller en extra ordinär händelse
- möjliggöra säkert informationsutbyte mellan verksamheter internt såväl som externt samt utgöra ett stöd för utveckling och digitalisering
- vara väl kommunicerat till verksamheterna genom att all personal fortlöpande ska få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande samt för att kunna leva upp till denna policy med tillhörande riktlinjer och instruktioner.

Årliga mål

Årliga mål ska formuleras i kommunens övergripande informationssäkerhetsplan. Målen ska baseras på en övergripande risk- och sårbarhetsanalys som i sin tur baseras på riskanalyser av verksamhetssystem och processer samt på omvärldsbevakning inom området. Målen ska också syfta till att för varje år förbättra ledningssystemets funktion och verkan.

Enligt GDPR artikel 30, ska varje personuppgiftsbehandling beskrivas i en registerförteckning som uppdateras löpande. Varje chef ska årligen kontrollera och intyga att den egna verksamhetens personuppgifts-behandlingar är registrerade och att registreringen stämmer med verkligheten. Övriga mål gällande dataskydd presenteras årligen i dataskyddsombudets årsrapport.

Aspekter och principer

Informationssäkerhetsaspekter

Konfidentialitet	att känslig och sekretesskyddad information inte röjs för obehörig och att informationen kan åtkomstbegränsas
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 det är möjligt att säkerställa vem som har lagt till, ändrat eller raderat information

Informationssäkerhet begränsas inte till säkerhet i verksamhetssystem utan omfattar information i alla dess former och oavsett hur informationen lagras, bearbetas och kommuniceras. Information kan till exempel 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.

Dataskyddsprinciper

Laglighet, korrekthet och öppenhet	Personuppgifterna ska behandlas på ett lagligt, korrekt (rimligt) och öppet sätt i förhållande till den registrerade.
Ändamålsbegränsning	Personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89 ska inte anses vara oförenlig med de ursprungliga ändamålen.
Uppgiftsminimering	Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas
Riktighet	Personuppgifterna ska vara riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål
Lagringsminimering	Personuppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning (GDPR) genomförs för att säkerställa den registrerades rättigheter och friheter.
Integritet och	Personuppgifterna ska behandlas på ett sätt som
konfidentialitet	säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.
Ansvarsskyldighet	den personuppgiftsansvarige ska ansvara för och kunna visa att punkterna ovan efterlevs

Roller och ansvar

I *Riktlinjer för informationssäkerhet* beskrivs ansvaret för samtliga roller i informationssäkerhetsarbetet mer detaljerat.

Informationssäkerhet

Kommunens nämnder är var och en ytterst ansvarig för hur information hanteras. Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten för informationen som hanteras i verksamheten.

Informationssäkerhetssamordnaren ansvarar för det stöd som är Ledningssystem för informationssäkerhet och dataskydd (LISD), framtagandet av informationssäkerhetsplan samt är rådgivande.

Dataskydd

Kommunens nämnder är var och en personuppgiftsansvarig enligt GDPR. Grundprincipen är att verksamheten utser en ansvarig chef för varje personuppgiftsbehandling (process).

Dataskyddsombudet är rådgivande och kontrollerande samt är kontaktperson gentemot allmänheten och Integritetsskyddsmyndigheten gällande dataskydd.

Verksamhetsdriven informationssäkerhet genom informationssäkerhetsklassning

Verksamheterna har själva ansvaret för sin informationssäkerhet och sitt dataskydd. De har också bäst kunskap om hur känslig och kritisk deras informationsmängder inklusive personuppgifter är och kan därmed bäst bedöma informationens skyddsvärde.

Verksamhetsdriven informationssäkerhet innebär att verksamheterna utifrån informationens skyddsvärde kan ställa krav på att de aktörer som direkt eller indirekt hanterar informationen, exempelvis kommunens IT-avdelning och externa systemleverantörer, gör det med tillräckliga säkerhetsåtgärder.

För detta ändamål ska informationssäkerhetsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Falu kommun ska tillämpa en enhetlig modell för informationssäkerhetsklassning som anger olika nivåer av skyddskrav. Informationen ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Verksamhetssystem och IT-infrastruktur

I de fall informationen hanteras digitalt är verksamheten tillsammans med IT-avdelningen, enligt beslutad systemförvaltningsmodell, ansvariga för drift och förvaltning av verksamhetssystem och lagringsytor. IT-avdelningen är ansvarig för att sätta standarden och utföra driften av kommunens egen IT-infrastruktur och IT-säkerhetsåtgärder. Verksamhetens utökade behov kring IT-infrastruktur och/eller IT-säkerhetsåtgärder sker i dialog med IT-avdelningen.

Förutsättningar

För att chefer och medarbetare ska kunna ta sitt ansvar för information och personuppgifter som hanteras i verksamheten behöver det säkerställas att kunskapen om offentlighetsprincipen och sekretessbestämmelser är tillräcklig.

För att chefer och medarbetare som ansvarar för verksamhetssystem ska kunna ta sitt ansvar behöver det säkerställas att det finns en implementerad samverkansmodell för verksamhetssystem och digitalt stöd.

Avvikelser

Varje medarbetare är skyldig att rapportera avvikelser[3] från denna policy och tillhörande riktlinjer och instruktioner. Avvikelserna rapporteras i incidentrapporteringssystemet och hanteras sedan enligt gällande process så att erfarenheter från dessa kan tas till vara som en del av ett kontinuerligt förbättringsarbete.

Granskning, uppföljning och rapportering

Informationssäkerhets- och dataskyddspolicyn med tillhörande riktlinjer och instruktioner ska granskas inför ledningens genomgång varje år och uppdateras om så krävs. Detta för att säkerställa styrdokumentens fortsatta lämplighet, riktighet och verkan. Granskningen ska inkludera en bedömning av kommunens möjligheter till förbättring av sitt regelverk och organisationens förhållningssätt till informationssäkerhet och dataskydd utifrån förändringar i omvärld, verksamhetsförutsättningar, legala krav och tekniska miljö.

Informationssäkerhetsamordnaren rapporterar till Kommunstyrelsen på ledningens genomgång i enlighet med LISD varje år.

Dataskyddsombudet utför årlig tillsyn av kommunens personuppgifts-hantering. Tillsynsresultat, rekommendationer samt plan för kommande tillsyn redovisas i dataskyddsombudets årsrapport under årets första kvartal.

Ansvar för policyn

Informationssäkerhetssamordnaren är ansvarig för granskning och uppdatering av policyn.

Kommunfullmäktige beslutar om policyn och nya versioner.

---

[3] En avvikelse kan vara en informationssäkerhetsincident, risk för informationssäkerhetsincident eller en personuppgiftsincident enligt artikel 33 i GDPR

Falu kommun, kommunikationskontoret, februari 2022 • Foto: Freepik

Falu kommun
023-830 00, Kontaktcenter
www.falun.se

FALUN