Falkenbergs kommun

Riktlinje – informationssäkerhet för medarbetare och förtroendevalda

Diarienummer 2019/538	Fastställt av Kommunstyrelsen	Datum för fastställande 2020-09-15
Dokumenttyp Riktlinje	Dokumentet gäller för Samtliga nämnder och bolag	Giltighetstid Tills vidare
Revideringsansvarig Kommunstyrelsen	Revideringsintervall Vart tredje år	Reviderad datum
Dokumentansvarig (funktion) Informationssäkerhetssamordnare	Uppföljningsansvarig och tidplan (se punkt 5) Respektive nämnd och bolag	

Falkenbergs kommun
311 80 Falkenberg. Telefon växel: 0346-88 60 00.
e-post: kontaktcenter@falkenberg.se
www.kommun.falkenberg.se

1. Syfte

Information är värdefullt och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen.

Varje dag hanterar kommunen mängder av information i olika former. Det kan vara information gällande elever, socialtjänst, livsmedelstillsyn eller stadsplanering och den kan förekomma i olika former: muntlig, skriftlig och/eller i IT-system.

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd utifrån behovet av informationens riktighet, tillgänglighet och konfidentialitet. Syftet med denna riktlinje är att underlätta för medarbetare och förtroendevalda att arbeta informationssäkert i vardagen.

Ytterst är det nämndens/ styrelsens ansvar att genom informationsspridning och kunskapshöjande insatser ge medarbetaren förutsättningar för en god informationssäkerhet.

Riktlinjen gäller för medarbetare, förtroendevalda och uppdragstagare verksamma inom Falkenbergs kommun.

2. Koppling till lagstiftning och andra styrdokument

Lagar och andra författningar är ett av samhällets starkaste styrmedel och fyller en viktig roll för att bygga upp informationssäkerhet både nationellt och internationellt. Denna riktlinje är förenlig med gällande lagstiftning och andra styrdokument.

Vad som ska betraktas som allmänna handlingar framgår av tryckfrihetsförordningens 2 kapitel. Huvudregeln är att allmänna handlingar är offentliga. Offentlighets- och sekretesslagen specificerar undantagen från denna huvudregel.

Uppgifter som är sekretessbelagda med hänsyn till Sveriges säkerhet ges ett särskilt skydd genom säkerhetsskyddslagen. Säkerhetsskyddet ska bland annat förebygga att sådana uppgifter på ett obehörigt sätt röjs, ändras eller förstörs samt hindra obehöriga att få tillträde till platser där de kan få tillgång till den typen av uppgifter.

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.

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.

Kommunens arkivreglemente utgår från arkivlagen, tryckfrihetsförordningen och Riksarkivets föreskrifter och anger hur kommunen arbetar med hantering av allmänna handlingar och arkivvård.

Kommunfullmäktige har antagit en informationssäkerhetspolicy som anger organisationens förhållningssätt till informationssäkerhetsarbetet. Riktlinje för hantering av personuppgifter i e-post och kalender beskriver närmare vilka personuppgifter som får hanteras i e-postklienten, idag Outlook.

3. Riktlinje

3.1. Medarbetares och förtroendevaldas ansvar för informationssäkerhet

Information är en viktig tillgång för Falkenbergs kommun. För att skydda informationen krävs ett medvetet säkerhetstänk hos alla medarbetare och förtroendevalda. Varje användare har sin del av ansvaret för säkerheten i informationshanteringen.

3.1.1. Behörighet

Falkenbergs kommuns informationssystem ska vara utrustade med behörighetskontrollsystem för att säkerställa att det endast är behöriga användare som kommer åt informationen.

De behörigheter medarbetaren/den förtroendevalda blir tilldelad ska bero på funktion, arbetsuppgifter/uppdrag och avgörs av närmsta chef och systemansvarig/förvaltare eller i samråd med systemansvarig/förvaltare. Behörigheter och lösenord är personliga och ska inte delas med kollegor. Undantag kan gälla för konton vid kiosker eller där många använder samma dator, dessa konton ska i så fall ha mycket begränsade behörigheter.

Varje medarbetare ansvarar för att följa de regler och riktlinjer som kopplas till behörigheten. Dessa regler kan vara utformade som styrande dokument, men också som regler/rutiner som delges i samband med tilldelning av behörighet till system eller dylikt. Allt som sker under behörigheten följer medarbetarens/den förtroendevaldas ansvar.

3.1.2. Inloggning

För att logga in i kommunens IT-system ska användar-ID och lösenord alternativt tvåfaktorsinloggning användas. Lösenord/pinkod är personliga och får inte göras kända för andra. Så fort datorn lämnas obevakad ska den låsas alternativt det smarta kortet/SITHS-

kortet dras ut och tas med. Varje nämnd/bolag kan fatta beslut om mer detaljerade anvisningar för kort och identifiering.

3.1.3. Incidenter

Incidenter ska anmälas och hanteras enligt respektive lagstiftning. Som exempel på lagstiftning som ställer särskilt krav på incidenthantering kan nämnas säkerhetsskyddslagen och lag om informationssäkerhet för samhällsviktiga och digitala tjänster (utifrån NIS-direktivet). Mer information kring anmälan av incidenter finns på respektive tillsynsmyndighets hemsida. Medarbetare ska rapportera incidenter till närmsta chef om inte särskild rutin anger annat.

Typ av incident	**Anmäls**	**Tillsynsmyndighet**
Identitetsstöld, eller misstanke om identitetsstöld	Till IT-service och närmsta chef. Notera/uppge när kontot senast använts och när incidenten upptäcktes.	
Personuppgiftsincidenter	Initialt via e-tjänst på intranät. Eventuellt vidare till tillsynsmyndigheten enligt rutin.	Datainspektionen
Incidenter som leder till störningar som får betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten enligt lag om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet).	Via anmälningsformulär på tillsynsmyndighetens hemsida och information på intranät. Endast särskilt utpekade sektorer omfattas av anmälningsplikten. Se definitioner och avgränsningar kap. 4	Myndigheten för samhällsskydd och beredskap
För verksamheter som omfattas av säkerhetsskyddslagen ska vissa typer av incidenter anmälas till Säkerhetspolisen.	Enligt information på Säkerhetspolisens hemsida.	Säkerhetspolisen.

3.1.4. Mobila enheter

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller bärbar (mobil).

- Mobila enheter som tillhandahålls av Falkenbergs kommun är personliga arbetsredskap som inte får lånas ut eller överlåtas om det inte är enheter som delas av flera.
- Uppsatta säkerhetsinställningar i enheter får inte ändras.
- Mobila enheter ska låsas med lösenord/pinkod eller motsvarande.
- Information som är känslig och/eller omfattas av sekretess får inte hanteras i smart telefon eller surfplatta.
- Viktig information bör inte lagras enbart på en bärbar enhet, utan snarast möjligt kopieras till anvisad lagringsplats i kommunens IT-miljö.
- Endast enhet som godkänts av kommunen och levererats av IT-service får anslutas till kommunens administrativa nät.
- Privat utrustning får endast anslutas till kommunens trådlösa gästnätverk.
- Förlust av enhet ska omedelbart anmälas till närmsta chef om inte annan rutin finns. Innehåller enheten personuppgifter ska anmälan göras i e-tjänst ”Anmälan av personuppgiftsincident”.

3.1.5. Skydd mot skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan infektera enheter, servrar eller nätverksutrustning.

- Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
- Var misstänksam och klicka inte på tveksamma länkar, fyll inte i irrelevanta uppgifter.
- Öppna bifogade filer endast om de kommer från betrodda och kända avsändare.
- Använd inte okända USB-minnen. Låt inte heller externa användare ansluta sina USB-minnen till kommunens administrativa nät (via datorer).
- IT-service skickar aldrig ut begäran av ID och lösenord, ignorera dessa e-postmeddelanden och radera dem. Anmäl händelsen till IT-service.

Om du misstänker att din enhet drabbats av skadlig kod, stäng omedelbart av enheten och kontakta IT-service.

3.1.6. Internetanvändning

Internet är för de anställda i Falkenbergs kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader eller risker för informationssäkerheten.

De regler som gäller i samhället i övrigt gäller även inom kommunen. Tryckfrihetsförordningen, brottsbalken, lag om upphovsrätt samt dataskyddsförordningen är exempel på lagar som måste beaktas när internet används.

Filmer, program och spel får inte för privat bruk laddas ned, strömmas, lagras eller spridas i eller via kommunens nätverk.

3.1.7. E-post

För många medarbetare/förtroendevalda är e-post det vanligaste och viktigaste sättet att förmedla information. Då är det viktigt att känna till att kommunikation via e-post normalt är helt öppen. Att skicka e-post från Falkenbergs kommun kan jämföras med att skicka vykort. För e-post gäller följande:

- Varje kontoinnehavare för ett personligt e-postkonto är ansvarig för den e-post som skickas från kontot.
- Ett e-postmeddelande som har kommit in till en tjänstemans e-postlåda och som rör myndighetens verksamhet är att anse som inkommet till myndigheten. Mot bakgrund av reglerna om allmänna handlingars offentlighet och om registrering av sådana handlingar måste inkomna e-postmeddelanden läsas löpande samt eventuellt tas om hand för registrering och ytterligare handläggning. Varje medarbetare ansvarar för att inkommen e-post handläggs enligt verksamhetens rutiner.
- Vid frånvaro, exempelvis semester, sjukdom eller föräldraledighet ska frånvaromeddelande aktiveras samt inkomna e-postmeddelande läsas löpande. Chef ansvarar för att planera för ersättare vid medarbetares frånvaro. Att använda ett frånvaromeddelande eller hänvisa till ersättare på plats är inte tillräckligt.
- E-post får inte automatiskt vidarebefordras till externa e-postadresser eller till den egna privata e-postadressen.
- E-postkonton som delas av flera, till exempel myndighetsbrevlådor och funktionsbrevlådor, ska ha utsedda ansvariga.
- Känslig information får inte kommuniceras via e-post. Se *Riktlinje för hantering av personuppgifter i e-post och kalender*.
- Det e-postkonto man fått i tjänsten får inte användas i privata syften, exempelvis för att öppna ett privat facebook-konto eller som kontaktuppgift i kundförhållanden till företag.

3.1.8. FollowMe

Kommunen använder utskriftssystemet ”FollowMe” på alla kopiatorer (MFP, Multifunktion printers). Det innebär att alla utskrifter ifrån stationära och mobila enheter lämnar skrivaren först när användaren är på plats vid kopiatorn och loggat in med sitt smarta kort/motsvarande såsom tagg eller passerkort. Detsamma gäller för kopiering.

Skanning av dokument skickas automatiskt till den inloggade användarens e-post. Tänk därför på att inte skanna dokument innehållande känslig information. Se *Riktlinje för hantering av personuppgifter i e-post och kalender*.

3.1.9. Klassificering av information

Klassificering av information är en förutsättning för att skapa rätt skydd för information av olika skyddsvärde. Som exempel kan nämnas behovet att skydda uppgifter i en patientakt i förhållande till konsekvenserna av att öppettiderna på biblioteket kommer i orätta händer.

Arbetet att klassa information pågår. Medarbetare/förtroendevalda ansvarar för att hantera informationen enligt informationsägarens instruktioner.

Varje förvaltning/bolag har en representant i nätverket för informationssäkerhet. Denna representant har extra kunskap om klassningsarbetet och kan svara på frågor från medarbetare och förtroendevalda.

3.1.10. Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av hårddiskkrasch, oavsiktlig radering eller som följd av krypteringsvirus.

- I väntan på ett ställningstagande kring lagring i molntjänster bör användning ske restriktivt och med försiktighet.
- Lagra ingen information på datorns lokala hårddisk, skrivbordet (C:).
- Information ska lagras på nätverket så att den säkerhetskopieras. I första hand ska information hanteras och/eller lagras i lämpligt verksamhetssystem. I undantagsfall kan lagring ske på din personliga hemkatalog (W:) och/eller gemensamma filareor (V:).
- Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska IT-service direkt kontaktas för försök att återskapa den senaste säkerhetskopian.
- Känsliga personuppgifter (särskilda kategorier av personuppgifter) och information som omfattas av sekretess får endast lagras i avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
- Känsliga uppgifter får inte lagras på USB-minnen för transport eller arkivering om de inte är krypterade eller åtkomstskyddade på annat sätt.
- Fysiska dokument som innehåller information som omfattas av sekretess ska förvaras i en av nämnden godkänd arkivskåp/arkivlokal. Nämnden kan i samband med detta rådgöra med kommunens arkivmyndighet (kommunarkivet). Mer information om arkivvård finns i kommunens arkivreglemente.
- Vid avslut av anställning eller vid byte till annan enhet ska datorer, telefoner eller andra enheter återlämnas till närmsta chef.
- Enheter som ska skrotas lämnas till IT-service kontor i stadshuset.

3.1.11. Säkert beteende

Oavsett vilka fysiska, tekniska och administrativa skydd som tillämpas krävs ett säkerhetsmedvetande hos samtliga medarbetare och förtroendevalda.

- Var försiktig när du hanterar känslig information och/eller information som omfattas av sekretess. Detta gäller i såväl offentliga miljöer som i vissa arbetssituationer.
- Så fort arbetsplatsen lämnas utan uppsikt ska datorn låsas. SITHS-kort/Smart kort ska alltid tas med då datorn lämnas.
- Pappersdokument innehållande känslig information och/eller information som omfattas av sekretess ska vid gallring strimlas eller kastas i godkända säkerhetskärl.

3.1.12. Avslutning av anställning

I samband med avslutning av anställning eller byte av tjänst ska följande åtgärder vidtas ur informationssäkerhetssynpunkt:

- Varje medarbetare/förtroendevald ansvarar för att se över vilken information som ska sparas, privat material tas bort.
- Vid byte av tjänst ska behörigheten följa respektive tjänst.
- Vid avslutning av anställning ansvarar närmsta chef för att samtliga behörigheter avslutas.
- Eventuella nycklar och taggar lämnas in. Detta är medarbetarens/den förtroendevaldes och chefens gemensamma ansvar. Smart kort/SITHS-kort och datorer med mera lämnas till närmsta chef.
- E-postkonto ska förses med frånvaromeddelande och avslutas 3 månader efter anställningens/uppdragets avslut.
- Personlig katalog (W:) avslutas 3 månader efter anställningens/uppdragets avslut.

4. Definitioner och avgränsningar

Med informationssäkerhet menas lämplig grad av administrativt och tekniskt skydd för all information oavsett bärare. IT-säkerhet ligger inom ramen för den tekniska informationssäkerheten. Med IT-säkerhet avses säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet.

Med känslig information avses känsliga personuppgifter (särskilda kategorier av personuppgifter i dataskyddsförordningen), personnummer, uppgifter om lagöverträdelser, uppgifter som omfattas av sekretess eller tystnadsplikt, skyddad identitet och adresser, lösenord och kontouppgifter.

En incident är en oönskad eller oplanerad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet. Exempel på incidenter kan vara

besökare på villovägar, misslyckad säkerhetskopiering, driftstörning eller försök till dataintrång.

Med incident enligt dataskyddsförordningen avses en händelse där en registrerad (invånare, anställd, förtroendevald) lider skada till följd av att känsliga uppgifter om denne läckt ut, ändrats, eller förstörts. Som exempel kan nämnas e-post som skickats till fel mottagare.

Mobil enhet avser i denna riktlinje bärbar dator, USB-minne, smart telefon och surfplatta.

Kommunens legitimerade personal, såsom sjuksköterskor och arbetsterapeuter, men också socialförvaltningens personal inom äldreomsorg använder SITHS-kort för åtkomst till nationella system med känslig information.
Merparten av övrig personal använder Smart kort för tvåfaktorsinloggning i datorer och anslutna verksamhetssystem/tjänster. Dessa kort används även för passersystem och utskriftssystemet ”FollowMe”.

Tjänster som omfattas av lag om informationssäkerhet för samhällsviktiga och digitala tjänster är indelade i sju sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, leverans och distribution av dricksvatten och digital infrastruktur.

Denna riktlinje innehåller information och regler gällande säkerhet vid all hantering av information inom kommunen.

Riktlinjen gäller för medarbetare, förtroendevalda och uppdragstagare verksamma inom Falkenbergs kommun.

Riktlinjen är underordnad den av fullmäktige antagna informationssäkerhetspolicyn. Detta innebär att det inte finns utrymme att besluta om lokala regler/anvisningar som avviker från policyn eller denna riktlinje.

5. Ansvar och uppföljning

Kommunstyrelsen ansvarar för att ta fram och revidera denna riktlinje. Ansvaret omfattar också att informera om riktlinjens innehåll och stödja verksamheterna i informationssäkerhetsarbetet.

Varje nämnd och styrelse ansvarar för informationssäkerheten inom respektive verksamhetsområde samt att denna riktlinje följs. I detta ansvar ligger att informera samtliga medarbetare, förtroendevalda och uppdragstagare om detta dokument samt följa upp efterlevnaden av riktlinjen.

Varje nämnd och styrelse kan vid behov fatta mer detaljerade anvisningar inom respektive verksamhet så länge det inte strider mot denna riktlinje.
Det är varje medarbetares och förtroendevalds ansvar att följa riktlinjen.