Falkenbergs kommun

Riktlinje – informationssäkerhet för medarbetare och förtroendevalda

Diarienummer KS 2023/354	Fastställt av Kommunstyrelsen	Datum för fastställande 2020-09-15
Dokumenttyp Riktlinje	Dokumentet gäller för Samtliga nämnder och helägda bolag	Giltighetstid Tills vidare
Revideringsansvarig Kommunstyrelsen	Revideringsintervall Vart tredje år	Reviderad datum 2023-12-05
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

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 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. Riktlinje

2.1. 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.

2.1.1. Behörighet

Behörigheter och inloggningsuppgifter är personliga och ska inte delas med kollegor. Undantag kan gälla för datorer som inte är anslutna till det administrativa nätet.

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. Medarbetaren/den förtroendevalda ansvarar för allt som sker under behörigheten.

2.1.2. Inloggning

Lösenord/pinkod är personliga och får inte göras kända för andra. Om datorn lämnas obevakad ska den låsas. Smart kort/SITHS-kort ska dras ut och tas med. Varje nämnd/bolag kan fatta beslut om mer detaljerade anvisningar för kort och identifiering.

2.1.3. Incidenter

Alla medarbetare är skyldiga att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på kommunens information. Det kan röra sig om exempelvis:

• IT-angrepp/intrång
• Skadlig kod
• Oskyddad känslig information
• Brister i efterlevnad av dessa riktlinjer för informationssäkerhet.

Incidenter rapporteras i anvisad kanal enligt särskild rutin, se nedan. Om en lagstadgad incidentrapportering görs ska kommunstyrelsen informeras.

Typ av incident	**Anmäls**	**Tillsynsmyndighet**
Identitetsstöld, eller misstanke om identitetsstöld. Exempelvis klickat på misstänkt länk.	Till IT-service via supportsidan och närmsta chef. Notera/uppge när kontot senast använts och när incidenten upptäcktes.	
Personuppgiftsincidenter, se Definitioner avsnitt 3.	Initialt via e-tjänst på intranät. Eventuellt vidare till tillsynsmyndigheten enligt rutin.	Integritetsskyddsmyndigheten
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 Myndigheten för samhällsskydd och beredskaps hemsida. Särskilt utpekade sektorer omfattas av anmälningsplikten.	Myndigheten för samhällsskydd och beredskap

2.1.4. 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.
- 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 utanför verksamhetssystem i smart telefon eller surfplatta.
- Viktig information bör inte lagras enbart på en bärbar enhet, utan snarast möjligt flyttas 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.
- Undvik USB-minnen. Risken att glömma bort vilken information som lagrats på USB-minnen och var USB-minnena finns är stor. Hantering av USB-minnen kräver spårbarhet vid överlämning och säker hantering i alla led. Se även 2.1.5.
- Förlust av enhet ska omedelbart anmälas till närmsta chef om inte annan rutin finns. Innehåller enheten personuppgifter ska händelsen hanteras enligt rutin för personuppgiftsincident, se 2.1.3.

2.1.5. 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.
- Undvik USB-minnen. Anslut aldrig upphittade/okända USB-minnen till kommunens administrativa nät. Låt inte externa användare ansluta sina USB-minnen till kommunens administrativa nät (via datorer). Se även 2.1.4.
- IT-service skickar aldrig ut begäran av ID och lösenord, ignorera dessa e-postmeddelanden. Anmäl händelsen till IT-service via anvisad kanal.

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

2.1.6. 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.

Som medarbetare är det bra att känna till att arbetsgivaren har rätt att under vissa förutsättningar granska medarbetarnas internetanvändning.

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

2.1.7. 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.
- En handling via e-post som har kommit in till en tjänstemans e-postlåda och som rör myndighetens verksamhet är att anse som inkommen 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.

2.1.8. Säker utskrift och skanning

Kommunen använder “Säker utskrift” på alla skrivare (MFP, Multifunktion printers). Det innebär att alla utskrifter ifrån stationära och mobila enheter lämnar skrivaren först när användaren är på plats vid skrivaren och loggat in med sitt smarta kort, eller motsvarande. Detsamma gäller för kopiering.

Öppen information skannas automatiskt till den inloggade användarens e-post. Känslig information skannas till inloggades hemkatalog på en skrivare med funktionen ”Säker skanning”. Kontakta verksamhetens personuppgiftssamordnare för att få information om vilken skrivare som har funktionen installerad.

2.1.9. Klassificering av information/Informationsklasser

Information är värdefullt och behöver skyddas efter behov. Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information.

Säkerhetsavdelningen ansvarar för att ta fram anvisningar för informationsklassning. Informationsägaren ansvarar för klassning av information.

Medarbetare/förtroendevalda ansvarar för att hantera informationen enligt informationsägarens instruktioner.

2.1.10. Lagring och säkerhetskopiering

Informationens skyddsvärde avgör vilka krav som gäller för säkerhetskopiering, lagringsytor och digital kommunikation. Ett beslut om lagringsplats ska därför föregås av informationsklassning, se 2.1.9. Säkerhetsavdelningen ansvarar för att ange och kommunicera lämpliga lagringsplatser.

- 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.
- Information som omfattas av sekretess samt känsliga personuppgifter (särskilda kategorier av personuppgifter) får endast lagras i avsedda och godkända system och lagringsytor med begränsad åtkomst. Begränsad åtkomst gäller för både användare och administratörer av systemet eller lagringsytan.
- Fysiska dokument som innehåller information som omfattas av sekretess ska förvaras i ett arkivskåp, eller arkivlokal, som nämnden godkänt. Nämnden kan i samband med detta rådgöra med 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 i stadshuset.

2.1.11. 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.
- Om 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.

2.1.12. 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 avslutning av anställning ansvarar närmsta chef för att samtliga behörigheter avslutas.
- Eventuella nycklar, kort och taggar lämnas in. Detta är medarbetarens/den förtroendevaldas och chefens gemensamma ansvar. Smart kort/SITHS-kort och datorer med mera lämnas till närmsta chef.

3. 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 exempelvis uppgifter som omfattas av sekretess eller tystnadsplikt, känsliga personuppgifter (särskilda kategorier av personuppgifter i dataskyddsförordningen), personnummer, uppgifter om lagöverträdelser, skyddad identitet och adresser, lösenord och kontouppgifter. Listan är inte uttömmande, information kan vara känslig utifrån andra aspekter.

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 personuppgiftsincident enligt dataskyddsförordningen avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Mobil enhet avser i denna riktlinje bärbar dator, USB-minne, mobiltelefon 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. Smart kort är ett alternativ för tvåfaktorsinloggning i datorer och anslutna verksamhetssystem/tjänster. Dessa kort används även för passersystem och ”Säker utskrift”.

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 säkerhetspolicyn. Detta innebär att det inte finns utrymme att besluta om lokala regler/anvisningar som avviker från policyn eller denna riktlinje.

4. Ansvar och uppföljning

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

Varje nämnd och bolagsstyrelse är ytterst ansvarig för informationssäkerheten inom sitt verksamhetsområde och kan vid behov 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, dataskydd, IT-säkerhet eller andra relaterade frågor fungerar som stöd i arbetet.

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

5. Koppling till lagstiftning och andra styrdokument

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

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

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