Riktlinje för informationssäkerhet

Dokumenttyp Riktlinje	Diarienummer KS 2024/837	Datum för beslut 2024-10-28	Version 2.0
Beslutsinstans Kommunstyrelsen	Dokumentansvarig Säkerhet och beredskapsavdelningen	Ansvarig för uppföljning Avdelningen för säkerhet och beredskap	Reviderad 2024-10-31
Dokumentet gäller Tillsvidare		Granskad av IT och digitaliseringsavdelningen	Aktualiserad -
Dokumentet gäller för			

Kommunkoncernen

Innehållsförteckning

1 Inledning

Kramfors kommun hanterar personuppgifter och annan känslig information som förutsätter en effektiv, rättssäker, insiktsfull och god hantering. För att säkerställa den enskilde individens integritet samt kommunens informationstillgångar arbetar kommunen systematiskt med övergripande säkerhets- och sekretessfrågor som en naturlig del i all verksamhet och i all utveckling.

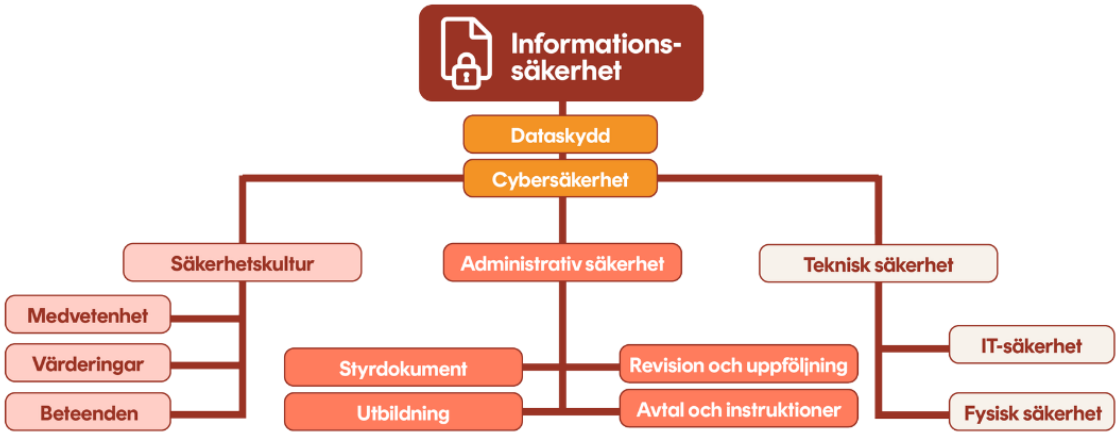
Denna riktlinje för informationssäkerhet anger hur Kramfors kommun arbetar med informationssäkerhet. Riktlinjen gäller för all verksamhet inom Kramfors kommun, inklusive de kommunala bolagen. Samtliga anställda, politiker och extern personal omfattas av riktlinjen.

2 Informationssäkerhet

Informationssäkerhet omfattar både dataskydd och cybersäkerhet. Dataskydd innebär att skydda informationstillgångar och säkerställa att de hanteras och lagras på ett sätt som är förenligt med gällande lagkrav. Dataskydd inkluderar grundläggande medvetenhet och kunskap hos medarbetarna samt systematiska administrativa och tekniska rutiner. Cybersäkerhet fokuserar på att skydda kommunens interna IT-infrastruktur från oönskad yttre påverkan, förhindra stöld av data och förhindra obehöriga intrång. För att upprätthålla hög nivå av dataskydd och cybersäkerhet integreras säkerhetskultur, administrativ säkerhet och teknisk säkerhet i vårt dagliga arbete.

Att bygga upp en säkerhetskultur innebär att skapa en medvetenhet och en attityd hos medarbetarna som främjar säkerhetsmedvetna beteenden och rutiner. Detta inkluderar utbildning, information och rutiner som tillsammans bygger en kultur där säkerhet är en naturlig del av det dagliga arbetet. Den administrativa säkerheten består av behörighetsstyrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. Den tekniska säkerheten inkluderar skydd av nätverk, servrar, arbetsstationer, hård- och mjukvara samt serverrum och utrymme för reservkraft eller säkerhetskopior.

Figur 1. Bild av hur informationssäkerhetsarbetets olika delar kan benämnas och hur de hänger ihop.



Källa: SKRs metodstöd för informationssäkerhetsarbete.

3 Systematiskt informationssäkerhetsarbete

Information är en av kommunens mest strategiska resurser och alla verksamheter är beroende av tillförlitlig information. Avbrott i tillgänglighet till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser för kommunens verksamhet.

Ledning och styrning av informationssäkerhetsarbetet konkretiseras i denna riktlinje för informationssäkerhet och i underliggande styrdokument. Kraven på informationssäkerheten utgår från ledningens och verksamhetens krav på funktion och tillämplighet liksom legala krav i lagar, förordningar och föreskrifter. Med ett systematiskt informationssäkerhetsarbete uppnås hög kvalitet och god effektivitet i det dagliga arbetet. Risken för störning ska minimeras samtidigt som skydd och åtgärder kontinuerligt balanseras mot kostnader. Insatser utgår från verksamhetens behov och är en del av kommunens arbete för att minska sårbarheter och öka verksamheternas robusthet och resiliens.

Informationssäkerhetsarbetet ska säkerställa att informationstillgångar skyddas utifrån informationstillgångens skyddsvärde oavsett om den hanteras manuellt eller digitalt.

Det systematiska arbetet med informationssäkerhet ska därför bedrivas i enlighet med den internationella informationssäkerhetsstandarden ISO/IEC 27000-serien, Ledningssystem för informationssäkerhet, och KLASSA ska användas för att klassificera information och säkerställa att rätt skyddsnivåer tillämpas. Kommunens informationstillgångar ska därför klassificeras enligt nedan:

- ***Tillgänglighet*:** Säkerställa att informationen är tillgänglig när den behövs för verksamheten.
- ***Riktighet*:** Informationen är tillförlitlig, korrekt, fullständig och inte manipulerad.
- ***Konfidentialitet*:** Förhindra obehörig åtkomst till informationen för att skydda känslig information.
- ***Spårbarhet*:** Möjliggöra spårning av vem som har haft åtkomst till informationen och vilka ändringar som har gjorts.
- ***Skydd mot förlust*:** Implementera åtgärder för att förhindra förlust av information, till exempel genom regelbundna säkerhetskopior.

Detta medför vidare att även IT-system klassificeras utifrån skyddsnivåer för IT-system utifrån kategorierna *Allvarlig, Betydande, Måttlig eller Försumbar.*

Kommunstyrelsen fastställer vilka system som är samhällsviktiga. Definitionen av samhällsviktiga system är de system som direkt eller indirekt hanterar den information som, vid ett bortfall eller en svår störning, kan leda till stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden. Dessa system ska genomgå en systemsäkerhetsanalys som utgör underlag för systemägares beslut om driftgodkännande.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna riktlinje.

3.1 Informationssäkerhetsplan

Tillämpningen av ovanstående metodstöd och vägledning, tillsammans med nedanstående punkter, tillser att Kramfors kommuns systematiska informationssäkerhetsarbete bidrar till att kommunen upprätthåller en nivå av informationssäkerhet som

- Grundar sig i ett riskbaserat arbetssätt.
- Tydliggör rutiner för incidentrapportering.
- Säkerställer robusthet och resiliens genom kontinuitetshantering.
- Innebär en säker och lagenlig informationshantering.
- Möjliggör digitaliseringssatsningar och underlättar transformering.
- Har en tillräcklig kompetensnivå.
- Bidrar till kvalitet och effektivitet.
- Bidrar till en hög säkerhetskultur och uppmuntrar engagemang hos samtliga medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten.

Informationssäkerhetsplanen innebär vidare att samverkan måste ske mellan systemägare och informationsägare eftersom många övergripande system innehåller information som har olika ägare och därmed även olika informationssäkerhetsklassningar.

4 Lagstiftning

Ramarna för Kramfors kommuns informationssäkerhetsarbete sätts utifrån gällande lagar och föreskrifter. Dessa beskriver de övergripande säkerhetskraven för verksamheten, inklusive hur information ska hanteras i datasystem. De säkerställer även att personlig integritet skyddas genom att sekretessbelagd information skyddas mot obehörig åtkomst.

Exempel på lagar:

- Offentlighets- och sekretesslag
- Tryckfrihetsförordningen
- Säkerhetsskyddslagen
- Säkerhetsskyddsförordningen
- Arkivlagen
- Allmänna dataskyddsförordningen
- NIS2 direktivet
- Lag om upphovsmannarätt till litterära och konstnärliga verk
- Lag om företagshemligheter
- Speciallagstiftning

Olika delar av kommunens arbete omfattas av olika grad av olika lagstiftning. Delar av kommunens arbete omfattas exempelvis av säkerhetsskyddslagstiftningen (se

tjänsteföreskrift säkerhetsskydd). För att en verksamhet eller tjänst skall omfattas av säkerhetsskyddslagen skall den ha bäring på något av de fyra skyddsvärdena, Sveriges yttre säkerhet, Sveriges inre säkerhet, nationellt samhällsviktig verksamhet eller skadegenererande verksamhet. Säkerhetsskydd består av personalsäkerhet, fysisk säkerhet och informationssäkerhet. Det övergripande systematiska informationssäkerhetsarbetet måste således ske i nära samverkan med de delar av verksamheten som berörs av säkerhetsskyddslagen.

5 Syfte med informationssäkerhetsarbete

Invånares och intressenters förtroende	• Informationssäkerhet ska bidra till att invånare och andra intressenter ska känna sig trygga vid informationsutbyte med kommunen och lita på vår förmåga att hantera informationstillgångar, till exempel personuppgifter.
Verksamhetens informations-säkerhet	• Samtliga anställda inom kommunens verksamheter ska ha kännedom och kunskap om aktuellt regelverk beträffande informationssäkerhet. • Verksamhetens systematiska arbete resulterar i en god informationssäkerhet som är anpassad efter verksamhetens förutsättningar och behov. • Det systematiska informationssäkerhetsarbetet ska minst omfatta informationsklassning, hot- och riskanalys, incidenthantering, kontinuitetsplaner samt uppföljning, åtgärder och återkoppling. • Om misstanke om oegentlighet uppstår ska detta utan fördröjning anmälas. • Oväntade händelser i IT-systemen som kan leda till negativa konsekvenser ska minimeras och förebyggas. • Investeringar och information ska skyddas i paritet med dess värde med beaktande av de negativa konsekvenser som otillräcklig säkerhet kan medföra. • Det ska finnas dokumentation av samtliga system.
Författningar	• Uppfylla de krav som ställs på informationssäkerheten i lagar, förordningar och föreskrifter.
Standarder	• Informationssäkerhet ska hanteras enligt den internationella standarden ISO/IEC 27000-serien. För att säkerställa att information klassificeras och att lämpliga skyddsnivåer tillämpas, ska Sveriges kommuner och regioners verktyg KLASSA och Myndigheten för samhällsskydd och beredskaps nationellt framtagna metodstöd användas.

Beredskapsplanering	• Hoten mot informationstillgångarna ska fortlöpande analyseras och informationssäkerheten ses som en del av kommunens kontinuitetsplanering i syfte att stärka förmågan att driva verksamheten vidare i händelse av en kris eller samhällsstörning.
Samhällsviktiga system	• Systemsäkerhetsanalys ska obligatoriskt genomföras. • Hotbilden ska löpande analyseras och följas upp och förebyggande åtgärder ska vidtas. • Samhällsviktiga system ska kontrolleras så att krishanteringsförmågan upprätthålls. • Allvarliga incidenter beträffande informationssäkerheten ska anmälas till informationssäkerhetssamordnare enligt särskild rutin.

6 Styrning av informationssäkerheten

Riktlinjen för informationssäkerhet är det övergripande dokumentet som styr kommunens informationssäkerhet. Riktlinjen anger informationssäkerhetens betydelse för kommunen och motsvarar den översta delen i pyramiden.

Tjänsteföreskriften för informationssäkerhet beskriver vad som behöver göras för att efterleva riktlinjen. Tjänsteföreskrifter motsvarar den mellersta nivån i pyramiden. I Kramfors kommun finns det ett flertal styrande dokument som har bäring på informationssäkerhet.

7 Organisation, roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att IT-system och tjänster kan administreras och hanteras på ett sådant sätt att de under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetsriktlinjens mål.

All information ska klassificeras utifrån dess krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Beroende på vilken klassificering som råder för en viss typ av information ska IT-system, tjänster, program och informationsmängder även klassificeras enligt MSB:s följande säkerhetsnivåer, allvarlig, betydande, måttlig och försumbar och förtecknas i systemöversikten för IT-system.

Ansvarig nämnd utser systemägare för de system som är förvaltningsspecifika. För gemensamma system utser kommunstyrelsen systemägare.

7.1 Organisation av informationssäkerhetsarbetet

- **Kommunstyrelsen** har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- **Informationssäkerhetssamordnaren** samordnar och utvecklar informationssäkerhetsarbetet.
- **Informationsägaren** är den som är ansvarig för sin information. Informationsägaren ansvarar för att information klassificeras i enlighet med (säkerhetskrav, klassa). Informationens klassificering avgör hur den ska hanteras, lagras och vem som har tillgång till den.
- **Systemägaren** har övergripande ansvar för respektive system och dess användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav. Systemens informationsmängder ska klassificeras.
- **Systemförvaltaren** har det funktionella helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet upprätthålls samt att planerade och beslutade aktiviteter genomförs i det dagliga arbetet. Systemförvaltare är tillika personuppgiftssamordnare för IT-system som behandlar personuppgifter.
- **IT och digitaliseringschefen** har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på IT-infrastrukturen. Arbetar i nära samverkan med informationssäkerhetssamordnare. IT-säkerhet är den miljö som faller under begreppet IT-infrastruktur. IT och digitaliseringschefen har även det yttersta ansvaret för att IT-system säkerhetsklassats enligt MSB:s säkerhetsklassningsnivåer.
- **Personuppgiftsansvarig**, det vill säga respektive nämnd och bolag, är ytterst ansvarig över hanteringen av personuppgifter. Ansvaret följer av lag och kan inte fördelas vidare.
- **Personuppgiftsbiträde** definieras som en fysisk eller juridisk person, offentlig myndighet eller annat externt organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

- **Personuppgiftssamordnare** är systemförvaltare för IT-system som behandlar personuppgifter och har som uppgift att stötta verksamheterna i ett aktivt arbete för att följa Dataskyddsförordningen.
- **Dataskyddsombud** ska övervaka efterlevnad av dataskyddsförordningen och annan lagstiftning som rör behandling av personuppgifter.
- **Alla** som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

8 Uppföljning

Arbetet med informationssäkerhet följs kontinuerligt upp i delårsuppföljningar och årsredovisning. Det pågående arbetet följs upp genom förvaltningsrapporter.