Kramfors kommun

Kommunledningsförvaltningen

Datum
2018-02-14

Riktlinje för informationssäkerhet

Dokumenttyp	Dokument-ID	Datum för beslut
Styrdokument	KS 2018/59	2018-04-23 § 42
Beslutsinstans	Dokumentansvarig	Ansvarig för uppföljning
Kommunfullmäktige	Säkerhets- och telekomstrateg	Säkerhets- och telekomstrateg
Dokumentet gäller tillsvidare		

Innehållsförteckning

1 Inledning

Medborgare, besökare och näringsliv i Kramfors kommun ska känna förtroende för den kommunala förvaltningen och vår förmåga till att utveckla samhället. Kramfors kommun tar tillvara på digitaliseringens möjligheter, vi stimulerar innovationer och använder oss av smarta e-tjänster som skapar direkta mervärden. Molntjänster, mobilitet, smarta telefoner och plattor med innovativa appar, sociala medier och tjänster skapar helt nya möjligheter för en ökad välfärd.

Med denna utveckling följer även nya hot och nya risker som ställer nya krav på kommunens förmåga att skydda och förvalta informationen på rätt sätt.

Kramfors kommun hanterar personuppgifter och annan känslig information som förutsätter en insiktsfull och god hantering. För att säkerställa den enskilde individens integritet arbetar kommunen aktivt med säkerhets- och integritetsfrågor som en naturlig del i all verksamhet och i all utveckling.

Denna riktlinje för informationssäkerhet anger hur Kramfors kommun arbetar med informationssäkerhet och uttrycker ledningens stöd för, och syn på, informationssäkerhet.

Denna riktlinje gäller för all verksamhet inom Kramfors kommun, inklusive de kommunala bolagen. Samtliga anställda, politiker och extern personal omfattas av riktlinjen och dess tillhörande tjänsteföreskrift med närmare instruktioner.

Informationssäkerhet omfattar alla kommunens informationstillgångar. Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild omfattas av informationssäkerhetsbegreppet.

2 Ledningens syn på informationssäkerhet

Riktlinjen för informationssäkerhet redovisar ledningens viljeinriktning och stöd för informationssäkerhetsarbetet och syftar till att klarlägga mål, organisation, ansvar och roller samt riktlinjer för områden av särskild betydelse. Informationssäkerhetsarbetet stödjer kommunens strategiska inriktning samt ingår som en del i kommunens process för ledning och styrning.

Information är en av kommunens mest strategiska resurser. 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 eller tredje part.

Ledning och styrning av informationssäkerheten konkretiseras i denna riktlinje för informationssäkerhet och underliggande styrdokument. Kraven på informationssäkerheten utgår från ledningens och verksamhetens krav på funktion och tillämplighet liksom legala krav, förordningar, föreskrifter, av-

tal och säkerhetskrav. Med rätt informationssäkerhet 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 totala riskhantering.

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.

Oavsett i vilken form informationen hanteras och av vem, så är det alltid den som äger informationen som har ansvaret för att informationen behandlas på ett ändamålsenligt och säkert sätt. Kramfors kommun följer etablerade standarder och vägledningar baserade på Svensk Standard för Informationssäkerhet enligt ISO 27000-serien. Samverkan måste ske mellan systemägare och informationsägare eftersom många övergripande system innehåller information som har olika ägare och därmed även olika säkerhetsklassningar.

Riktlinjen ska, av chef eller motsvarande, kommuniceras till samtliga anställda vid nyanställning samt när riktlinjeen är ny eller reviderad. Den ska vara känd och tillgänglig i aktuell version på kommunens intranät Portalen och på kommunens hemsida.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna riktlinje. Riktlinje för informationssäkerhet ska fastställas i kommunfullmäktige.

3 Bakgrund

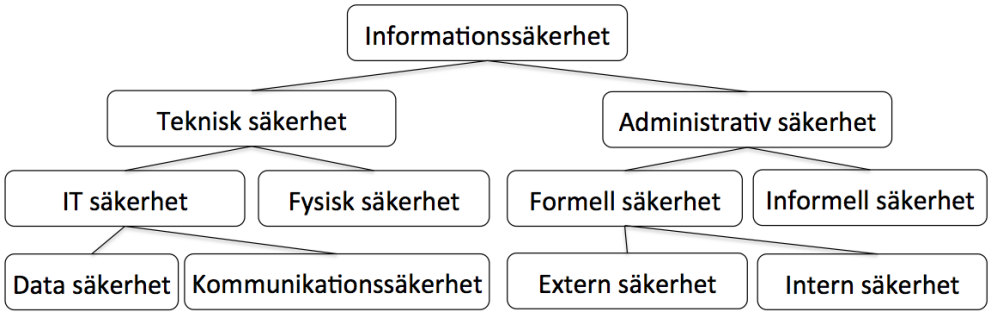
Kommunens alla verksamheter är beroende av att information är tillgänglig för rätt person vid rätt tidpunkt, att den är korrekt och riktig samt utgör ett bra verksamhetsstöd. Eftersom det finns många hot mot våra informationstillgångar är informationssäkerhet mycket viktigt. Information uttrycker kunskap och är en tillgång för individer och organisationer. Vi kan kommunicera information, vi kan lagra den, vi kan styra processer med den – vi behöver den för det mesta vi gör helt enkelt. För att säkerställa att informationen är skyddad finns det särskilda informationssäkerhetskrav som behöver uppfyllas.

Med informationssäkerhet avses skydd av informationstillgångar i syfte att upprätthålla nödvändig nivå på sekretess, riktighet, tillgänglighet och spårbarhet.

- Sekretess/Konfidentialitet - att information skyddas mot obehörig insyn och åtkomst

- Riktighet – att information är tillförlitlig, korrekt och fullständig och inte manipulerad eller förstörd
- Tillgänglighet– att information är nåbar för rätt person vid rätt tillfälle
- Spårbarhet – att det går att följa hur och när informationen har hanterats och kommunicerats

Enkelt uttryckt kan informationssäkerhet delas upp i två delar. Den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet. Här återfinns nätverk, servrar, arbetsstationer, hård- och mjukvara samt serverrum och utrymme för reservkraft, säkerhetskopior etcetera. Bilden nedan illustrerar skillnaden på administrativ och teknisk säkerhet.



Den tekniska säkerheten förutsätter att det finns en administrativ säkerhet för att rätt tekniska åtgärder ska kunna vidtas. IT-säkerhet är alltså en del av informationssäkerhetsbegreppet.

4 Lagstiftning

Ramarna för Kramfors kommuns informationssäkerhetsarbete sätts utifrån gällande lagar och föreskrifter. Dessa anger bland annat de övergripande säkerhetskrav som ställs på verksamheten och därmed även på hanteringen av information i datasystem, vilket bland annat reglerar skyddet av den personliga integriteten

- att sekretessbelagd information ska skyddas mot otillbörlig åtkomst, med iakttagande av offentlighetsprincipen, samt
- olika intressenters krav på korrekt information och allmänhetens lagliga rätt till insyn i offentliga handlingar

Exempel på lagar:

- Offentlighets- och sekretesslag (2009:400)
- Tryckfrihetsförordningen (SFS 1949:105)
- Säkerhetsskyddslagen (SFS 1996:627)
- Säkerhetsskyddsförordningen (SFS 1996:633)
- Arkivlagen (1990:782)

- Personuppgiftslagen (SFS 1998:204) gäller till 2018-05-25
- Allmänna dataskyddsförordningen, GDPR (EU 2016/679) gäller från 2018-05-25
- Lag om upphovsmannarätt till litterära och konstnärliga verk (SFS1960:729)
- Lag om skydd av företagshemligheter (SFS 1990:409)
- Speciallagstiftning

5 Grundläggande mål för informationssäkerhets-arbetet

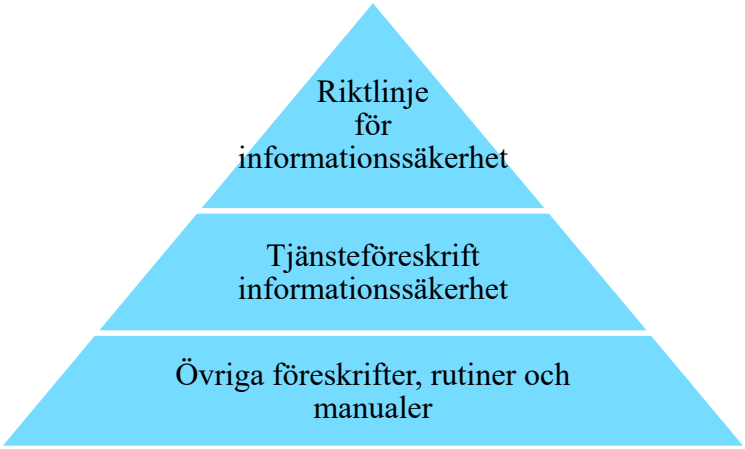
Kramfors kommuns informationssäkerhetsarbete syftar till att uppfylla följande mål.

Medborgares och intressenters förtroende	• Informationssäkerhet ska bidra till att medborgare och andra intressenter ska känna sig trygga vid informationsutbyte med kommunen och 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. • Grunden för ett systematiskt 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	• Arbetet med informationssäkerhet ska följa ISO 27000-standarden. ISO 27000 är en internationellt erkänd standard för informationssäkerhet framtagen och verifierad av experter runt om i världen.
Krishantering	• Hoten mot informationstillgångarna ska fortlöpande analyseras och informationssäkerheten ses som en del av kommunens krishantering 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. • 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. Ett exempel är att ledningen uttrycker att information ska vara tillgänglig och återläsningsbar.



Tjänsteföreskriften beskriver vad som behöver göras för att efterleva riktlinjen. Tjänsteföreskriften motsvarar den mellersta nivån i pyramiden. Ett exempel på innehåll i tjänsteföreskrift är till exempel att säkerhetskopiering ska genomföras. Återläsningsrutiner som när och för hur lång tid detta ska vara möjligt dokumenteras i överenskommelser mellan systemägare och IT-enheten.

Baserat på tjänsteföreskrifterna om informationssäkerhet och systemförvaltning utformas instruktioner och anvisningar som anger hur rutiner och säkerhetslösningar ska utformas och tillämpas för olika verksamhetssystem. Den samlade dokumentation tillsammans med de processer som ingår i ett systematiskt informationssäkerhetsarbete utgör ett ledningssystem för 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 (sekretess), riktighet och tillgänglighet. Information relaterad till hälso- och sjukvård ska även klassas utifrån krav på spårbarhet. Beroende på vilken klassificering som råder för en viss typ av information ska IT-system, tjänster, program och informationsmängder vara identifierade och förtecknade.

Respektive nämnd utser systemägare och informationsägare för de system och register som är förvaltningsspecifika. För gemensamma system utser kommunstyrelsen system- och informationsägare. En särskild tjänsteföreskrift för systemförvaltning kommer att finnas och även en för personuppgifter och behörigheter.

7.1 Organisation av informationssäkerhetsarbetet

- **Kommunfullmäktige** uttrycker sin viljeinriktning i denna.
- **Kommunstyrelsen** har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- **Informationssäkerhetssamordnaren** har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.
- **Närmaste chef** ansvarar för att det finns rutiner som säkerställer en god efterlevnad av kommunens regelverk för informationssäkerhet.
- **Informationsägaren** har det övergripande och yttersta ansvaret för sin information. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem.
- **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 utfö-

rare och ser till att systemets funktionalitet upprätthålls samt att planerade och beslutade aktiviteter genomförs i det dagliga arbetet.

- **IT-chefen** 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.
- **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** 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

Kommunstyrelsen ska minst en gång per år informera sig om hur arbetet med informationssäkerhet pågår i kommunens förvaltningar. Genomgången görs vid den årliga aktiviteten ”ledningens genomgång”.

Uppföljningen ska baseras på underlag med rekommendationer som tas fram av informationssäkerhetssamordnaren.

Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten
- Utbildning (status och behov)
- Inträffade incidenter av större påverkan på verksamheten
- Resultat från genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till förbättringar

Resultatet från denna uppföljning ska innefatta beslut om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser.

I de fall regler inte följs kan följden bli disciplinära åtgärder. Om man kan förmoda att brott mot lag har begåtts lämnas information till brottsutredande myndighet.