Riktlinjer för informationssäkerhet

Dokumentnamn Riktlinjer för informationssäkerhet		Antagen	Beslutsinstans Kommunstyrelsen
Dokumenttyp Riktlinje	Diarienummer KS 2023-00330	Ersätter -	Gäller från och med

1 Inledning

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i det dagliga arbetet. Det grundläggande och övergripande dokumentet för kommunens arbete med informationssäkerhet är informationssäkerhetspolicyn. Policyn fastställs av kommunfullmäktige. Denna riktlinje avser att konkretisera den av fullmäktige fastställda *Informationssäkerhetspolicyn*[1] för att uppnå kommunfullmäktiges mål och viljeinriktning.

Utöver denna riktlinje tillkommer också områdesspecifika riktlinjer och rutiner. Vägledande och normerande i kommunens arbete med informationssäkerhet ska vara Myndigheten för samhällsskydd och beredskaps (MSB) *Metodstöd för systematiskt informationssäkerhetsarbete.*

2 Mål

Kommunfullmäktiges mål är att genom ett transparent och systematiskt informationssäkerhetsarbete:

- förhindra att skyddsvärd information hamnar i orätta händer,
- säkerställa att rätt information finns tillgänglig för rätt person vid rätt tillfälle,
- förhindra eller minska effekter av störningar och skador,
- upprätthålla den personliga integriteten,
- upprätthålla ett högt förtroende hos medborgarna.

Ovannämnda mål är att betrakta som långsiktiga mål för verksamheten. Vidare är målen att betrakta som ett led i kommunens arbete för att uppfylla de krav som lagstiftningen ställer på verksamheten.

3 Aktiviteter

Kommunchef fastställer årligen en övergripande handlingsplan. Handlingsplanen tydliggör hur förvaltningen går från behov till faktisk åtgärd. Handlingsplanen syftar till att eliminera eller reducera de risker och brister som identifierats.

4 Roller och ansvarsfördelning

Grundprincipen är att ansvaret för informationssäkerhetsarbetet följer det ordinarie verksamhetsansvaret. Det innebär att den som är ansvarig för ett visst verksamhetsområde också är ansvarig för själva informationssäkerheten inom det specifika området.

[1] Fastställd av kommunfullmäktige 2022-06-20.

4.1 Informationssäkerhetssamordnare

Det ska finnas en utpekad stödfunktion (informationssäkerhetssamordnare) med uppdrag att leda och samordna arbetet med informationssäkerhet i förvaltningen. Denna stödfunktion ansvarar således inte för informationssäkerheten som sådan, men ansvarar däremot för att inom informationssäkerhetsområdet bland annat:

- **Analysera omvärlden och den egna organisationen**.
- **Utveckla informationssäkerhetsarbetet**, genom att exempelvis utforma och förvalta styrande dokument, modeller, standarder och mallar.
- **Stödja förvaltningen** att efterleva, genomföra och använda utformade styrande dokument, modeller med mera. Till exempel genom olika metoder, vägledningar, utbildningar, kravställningar och konkret deltagande.
- **Kontrollera och följa upp** arbetet.

4.2 Övriga roller

Övriga aktuella roller inom ramen för kommunens arbete med informationssäkerhet beskrivs i *Systemförvaltning i Vansbro kommun*.

5 Informationstillgångar

Begreppet information innefattar såväl digital som analog, oaktat om den behandlas manuellt eller automatiserat. Skyddsvärd information benämns informationstillgångar, vilket också inkluderar de resurser som behandlar informationen, som exempelvis IT-system, databaser, datorer, bildskärmar, surfplattor och telefoner. En informationstillgång kan vara av fysisk eller logisk karaktär, eller bådadera.

6 Informationens struktur

Alla som arbetar med att framställa, registrera, bevara och skydda kommunens informationstillgångar berörs av hur informationen systematiseras och hanteras. Det är många roller som gemensamt måste hjälpas åt att säkra upp och göra informationen användbar nu och i framtiden. För att uppnå detta krävs struktur. Kommunens information ska struktureras och beskrivas enligt den processorienterade och organisationsoberoende klassificering som avser kommunala verksamheter och benämns *Klassa*[2].

Närmare bestämmelser om klassificeringsstrukturen fastställs inom förvaltningen.

6.1 Arkiv

Bestämmelser kring kommunens arkivbildning och gallring framgår av arkivlagen (1990:782). Ett arkiv bildas i huvudsak av respektive myndighets allmänna handlingar.

De allmänna handlingar som myndigheten inte längre har behov av ska gallras alternativt överlämnas till arkivmyndigheten[3] för slutarkivering.

[2] Klassa är framtagen inom Samrådsgruppen för kommunala arkivfrågor med huvudmännen Sveriges Kommuner och Regioner (SKR) samt Riksarkivet.
[3] Kommunstyrelsen är tillika arkivmyndighet i Vansbro kommun.

De allmänna handlingar som överlämnats till arkivmyndigheten tas omhand i kommunarkivet. Kommunarkivet består dels av ett fysiskt arkiv men också ett digitalt arkiv.

Allmänna handlingar som upprättats eller inkommit fram till och med år 2017, ska struktureras i enlighet med allmänna arkivschemat. Allmänna handlingar som härrör till ärenden skapade under samma period ska också struktureras enligt allmänna arkivschemat, även om de inkommit eller upprättats efter denna tidpunkt. Allmänna handlingar som tillkommit efter år 2017 ska struktureras enligt den processorienterade klassificeringsstrukturen som framgår av föregående avsnitt.

De allmänna handlingar som från och med verksamhetsåret 2024 överlämnas till arkivmyndigheten för slutarkivering, ska överlämnas i digitalt format för digitalt bevarande. Undantag gäller för de allmänna handlingar som på grund av juridiska hinder eller handlingar vars autencitet inte kan överföras till digital form. Exempel på detta kan vara handlingar innehållande vattenstämpel eller egenhändig underskrift. Riksarkivets föreskrifter ska för detta vara normerande.

Arkivering enligt föregående stycke föregås av beslut från arkivmyndigheten.

7 Informationshanteringsplan

I enlighet med kommunens arkivreglemente[4] ska en plan upprättas som beskriver myndighetens[5] handlingar och huruvida de ska bevaras eller gallras. Detta görs i en bevarandeplan som fastställs av respektive myndighet.

Som framgår av avsnitt 8.1 nedan ska respektive myndighet föra ett register över sina personuppgiftsbehandlingar. Detta register benämns Artikel 30-register (dataskydd).

I enlighet med avsnitt 10 nedan ska respektive myndighet värdera sin information utifrån vilka konsekvenser ett otillräckligt skydd skulle kunna få. Detta görs genom informationssäkerhetsklassning.

Den sammantagna informationen av dessa tre delar ordnas i en informationshanteringsplan.

Närmare bestämmelser om vilka uppgifter som framgår av informationshanteringsplanen fastställs inom förvaltningen.

8 Dataskydd

En del av kommunens arbete med informationssäkerhet innefattar den om dataskydd. Med dataskydd förstås kommunens behandling av personuppgifter och de åtgärder som vidtas för att upprätthålla den personliga integriteten.

Kommunens verksamheter har att vid all behandling av personuppgifter säkerställa att behandlingen sker inom ramen för gällande lagstiftning, det vill säga dataskyddsförordningen med tillhörande författningar. Vidare ska verksamheterna säkerställa att dokumentation finns

[4] Fastställt av kommunfullmäktige 2013-12-19.
[5] Förstås som kommunstyrelsen och övriga nämnder, kommunfullmäktiges revisorer samt andra kommunala organ med självständig ställning. Se kommunens arkivreglemente för definition.

som beskriver på vilket sätt lagstiftningen följs och vilka avvägningar som gjorts för att följa den.

I tillämpliga fall ska Sveriges Kommuners och Regioners (SKR) utarbetade mallar och blanketter ses som normerande för utformningen av kommunens dito.

8.1 Artikel 30-register

Som personuppgiftsansvarig ska kommunens respektive myndigheter föra register över sina personuppgiftsbehandlingar. Registret ska upprättas skriftligen, vara tillgängligt i elektroniskt format och hållas uppdaterat. Innehållet i registret framgår av artikel 30 i dataskyddsförordningen.

Närmare bestämmelser om registret och dess utformning fastställs inom förvaltningen.

8.2 Konsekvensbedömning

En konsekvensbedömning är en process för att ta reda på vilka risker som finns med att behandla personuppgifter, men även en process för att ta fram rutiner och åtgärder för att bemöta dessa risker.

Alla personuppgiftsbehandlingar kräver inte att en konsekvensbedömning görs. Initialt görs en analys av de risker behandlingen kan innebära samt vilka åtgärder som kan vara lämpliga att vidta. Om behandlingen därefter sannolikt leder till en hög risk för enskilda personers fri- och rättigheter genomförs en konsekvensbedömning. I tveksamma fall görs en konsekvensbedömning.

Om utfallet från konsekvensbedömningen fortsatt innebär en hög risk för enskilda personers fri- och rättigheter ska verksamheten samråda med tillsynsmyndigheten[6] innan behandlingen påbörjas, ett så kallat förhandssamråd.

Närmare bestämmelser om tillvägagångssätt och dokumentation av konsekvensbedömningar fastställs inom förvaltningen.

8.3 Registrerades rättigheter

De individer vars personuppgifter behandlas har ett antal rättigheter i enlighet med dataskyddslagstiftningen. Dessa rättigheter framgår främst av dataskyddsförordningens 3:e kapitel.

Förvaltningen har att utarbeta rutiner, arbetssätt och blanketter för att kommunen ska kunna tillgodose enskilda individers samtliga rättigheter.

8.4 Personuppgiftsbiträdesavtal

Om kommunen anlitar någon utanför kommunens organisation att för kommunens räkning behandla personuppgifter, är den kommunens personuppgiftsbiträde. I de fall kommunen agerar personuppgiftsbiträde åt någon annan, exempelvis vid samverkan med andra kommuner, gäller omvänt avtalsförhållande.

[6] Integritetsskyddsmyndigheten

Relationen mellan personuppgiftsansvarig och personuppgiftsbiträde regleras i ett skriftligt personuppgiftsbiträdesavtal. Avtalet ska säkerställa att:

- båda parter följer dataskyddsförordningen,
- båda parter är medvetna om sina åtaganden och skyldigheter mot varandra och de registrerade,
- båda parter skyddar kunders, personals och andra kategorier av registrerades personuppgifter,
- båda parter dokumenterar tydligare och därmed kan visa att de följer reglerna (ansvarsskyldighet).

Den mall för personuppgiftsbiträdesavtal, med tillhörande instruktioner, som Sveriges Kommuner och Regioner (SKR) tillhandahåller ska vara normerande för de personuppgiftsbiträdesavtal som kommunen ingår.

Process och dokumentation vid ingående av personuppgiftsbiträdesavtal fastställs inom förvaltningen.

8.5 Hantering av personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Enligt artikel 33 i dataskyddsförordningen ska en personuppgiftsincident anmälas till Integritetsskyddsmyndigheten om det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

För övriga personuppgiftsincidenter gäller att de ska dokumenteras.

Kommunens hantering av personuppgiftsincidenter ska koordineras med den incidenthantering som avser övriga informationssäkerhetsincidenter.

9 Säkerhetsskydd

Den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet har att följa säkerhetsskyddslagstiftningen.

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Med säkerhetsskydd avses att skydda uppgifter som är av betydelse för Sveriges säkerhet, mot till exempel spioneri, terroristbrott eller sabotage.

9.1 Säkerhetsskyddsanalys och säkerhetsskyddsplan

Kommunen ska utreda behovet av säkerhetsskydd i en säkerhetsskyddanalys. Analysen ska dokumenteras.

Utifrån vad som framkommit i säkerhetsskyddsanalysen ska en säkerhetsskyddsplan upprättas. Planen ska redogöra för hur behovet av säkerhetsskyddsåtgärder[7] som identifierats i analysen omhändertas. Det ska vidare framgå när åtgärderna vidtas och vilken funktion som ansvarar för dem.

9.2 Säkerhetsprövning

Den som genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas, och i förekommande fall säkerhetsklassas. Prövningen syftar till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt.

Säkerhetsprövningen ska dokumenteras. Riktlinjer och rutiner som närmare reglerar säkerhetsprövning och säkerhetsklassning fastställs på behörig nivå.

9.3 Incidenthantering avseende säkerhetsskydd

En incident enligt säkerhetsskyddslagstiftningen är en typ av säkerhetshotande händelse. Den kan bero på såväl ett avsiktligt som oavsiktligt agerande av egen personal eller av en hotaktör.

Förvaltningen har att säkerställa att rutiner för hantering av säkerhetshotande händelser (incidenthanteringsplan) är utarbetade. Förvaltningen ska också säkerställa att det finns utpekad personal som har att verkställa planen.

Kommunen ska skyndsamt anmäla till Säkerhetspolisen om en incident inträffat i enlighet med säkerhetsskyddsförordningen (2018:658) 2 kap. 10 §.

9.4 Dokumentationskrav

Bedömningar, beslut, planer och åtgärder samt uppföljning enligt säkerhetsskyddslagstiftningen ska dokumenteras.

10 Informationssäkerhetsklassning[8] (konsekvensnivåer)

Informationssäkerhetsklassning innebär ett enhetligt sätt att värdera information utifrån vilka konsekvenser ett otillräckligt skydd skulle kunna få. Konsekvenserna delas upp i ett antal nivåer (konsekvensnivåer).

För att nå enhetlig värdering upprättas en klassningsmatris med tillhörande stödmaterial. Antalet konsekvensnivåer och definitionen av dem fastställs inom förvaltningen.

[7] Säkerhetsskyddslagen (2018:585) indelar dessa i områdena *informationssäkerhet, fysisk säkerhet* samt *personalsäkerhet.*
[8] Myndigheten för samhällsskydd och beredskap benämner detta *Informationsklassning*.

Kommunfullmäktige fastställer i *Informationssäkerhetspolicy* vilka aspekter som avses och ska användas vid informationssäkerhetsklassningen. Dessa innefattar *konfidentialitet, riktighet* och *tillgänglighet.*

11 Riskhantering

Informationssäkerhetsrisker, det vill säga risker som kan kopplas till verksamhetens **informationstillgångar**, ska beskrivas och analyseras.

Den modell som används för att beskriva och analysera risker ska verka för en enhetlig värdering över samtliga verksamheter. Riskanalysmodellen fastställs inom förvaltningen.

12 Informationssäkerhet (säkerhetsåtgärder)

För att nå kommunfullmäktiges mål avseende informationssäkerhet behöver verksamheten, efter att den beskrivit identifierade risker och konsekvenser, införa tillräckliga säkerhetsåtgärder.

Vid bedömningen av vilka säkerhetsåtgärder som ska implementeras behöver man värdera vilka säkerhetsåtgärder som kan ge ett tillräckligt skydd och samtidigt vara kostnadseffektivt.

12.1 Områden för säkerhetsåtgärder

12.1.1 Administrativ

Administrativa säkerhetsåtgärder innefattar upprättande av styrande dokument och rutiner eller utbildningar som stöd för en säker informationshantering.

12.1.2 Fysisk

Fysiska säkerhetsåtgärder innefattar bland annat att ha lås och larm som skyddar informationstillgångar mot obehörig fysisk åtkomst. Det innefattar även åtgärder så som brandskydd, kyla och fysiskt separerade servermiljöer.

12.1.3 Organisatorisk

Organisatoriska säkerhetsåtgärder innefattar fördelning av ansvar, roller och mandat i organisationen för att skydda mot att informationen hanteras felaktigt.

12.1.4 Teknisk

Tekniska säkerhetsåtgärder avser olika IT-lösningar som används för att skydda information. Exempel på detta kan vara antivirus, behörighetssystem, säkerhetsloggning och säkerhetskopiering.

12.2 Skyddsnivåer

För varje konsekvensnivå (beskrivet under avsnitt 8) finns en skyddsnivå. Skyddsnivå är en samling säkerhetsåtgärder som ger ett tillräckligt skydd för information klassat till en given konsekvensnivå.

Syftet med att samla säkerhetsåtgärder i nivåer är att underlätta förvaltningen av säkerhetsåtgärderna och bidra till förståelsen för vilka säkerhetsåtgärder som är aktuella för vilka konsekvensnivåer.

Antalet skyddsnivåer och vad dessa innehåller fastställs inom förvaltningen.

13 Incidenthantering avseende informationssäkerhet

En informationssäkerhetsincident definieras som *en oönskad händelse med negativa konsekvenser för kommunens informationstillgångar, alternativt en oönskad sårbarhet med potentiellt negativa konsekvenser för kommunens informationstillgångar*.

Incidenthanteringen syftar till att förbättra kommunens förmåga att

- minimera risken för att incidenter uppstår,
- minska konsekvenserna av dem,
- utreda orsakerna till att de kunnat ske, och därigenom förbättra skyddet så att liknande incidenter inte inträffar i framtiden.

Identifierade incidenter ska dokumenteras enligt en systematik och koordineras med den incidenthantering som avser personuppgifter. Förvaltningen ansvarar för att upprätta ett arbetssätt som möjliggör detta.

14 Förvaltning av system

Olika typer av IT-stöd används i så gott som samtliga kommunens verksamheter. IT-stöden innehåller ofta stora mängder information. För att borga för en trygg hantering av informationstillgångarna krävs en systematisk förvaltning av respektive IT-stöd. Den systematiska förvaltningen av IT-stödet dokumenteras i en förvaltningsplan. Innehållet och utformningen av sådana planer fastställs inom förvaltningen.

15 Kontinuitetshantering för informationstillgångar

Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet[9] på en tolerabel nivå oavsett vilken störning den utsätts för. Kontinuitetsplaneringen bidrar till att verksamheten snabbare kan återhämta sig från och mildra konsekvenserna av en inträffad störning.

Kontinuitetshantering för informationstillgångar ingår i, och dokumenteras tillsammans med, kommunens ordinarie kontinuitetsplanering.

16 Utbildning

Varje anställd som hanterar kommunens informationstillgångar ska ges en grundläggande utbildning inom informationssäkerhet och dataskydd.

Dessutom ska kommunens anställda ges vidare utbildning på områdena i den mån uppdraget kräver detta.

17 Uppföljning och förbättringsarbete

Kommunens informationssäkerhetsarbete ska präglas av ständiga förbättringar och består av flera delar.

[9] Primärt verksamhetens grunduppdrag.

17.1 Handlingsplan

En del i detta är fastställande av en handlingsplan som gäller för området. Handlingsplanen syftar till att tydliggöra hur organisationen går från behov till faktisk åtgärd, det vill säga att eliminera eller reducera de informationssäkerhetsrelaterade risker och brister som identifierats.

Handlingsplanen innehåller årliga mål med därtill hörande årliga aktiviteter och gäller årsvis eller fram till dess att en ny handlingsplan fastställts.

Uppföljning av handlingsplanen med aktiviteter görs kontinuerligt.

17.2 Intern kontroll

Vidare består förbättringsarbetet av kontrollpunkter i den interna kontrollplan som årligen fastställs. Eventuella brister som framkommer i uppföljningen av planen analyseras och vid behov, åtgärdas.