Älvkarleby kommun

Informationssäkerhets- och dataskyddspolicy

Älvkarleby kommun

Antagen av: Kommunfullmäktige , 2023-02-15
Senast reviderad:
ÄKF-nummer:
Handläggare/författare: Joel Gordon Hultsjö , Arkivarie & Informationssäkerhetssamordnare
.

Älvkarleby
kommun

Älvkarleby kommun

Innehåll

Inledning

I det digitala samhället kan ingen verksamhet upprätthållas utan en fungerande informationshantering. Därmed är kommunens informationshantering en verksamhetskritisk resurs. Bristfällig informationssäkerhet leder till bland annat risk för liv och hälsa och för den personliga integriteten, men även risk för stark negativ ekonomisk påverkan och för att tilliten till kommunen skadas.

Informationssäkerhetsarbetet ska bidra till att kommunens nämnder och av kommunen majoritetsägda bolag kan genomföra samtliga uppdrag utan störningar samt skapa en motståndskraft och förmåga till återhämtning i de fall störningar inträffar.

Älvkarleby kommuns mål för dataskydd är att all behandling sker med hänsyn till den enskildes friheter och rättigheter. Innebörden i detta är att värna om den personliga integriteten genom att medborgare och anställda är trygga i att kommunen eftersträvar att alltid sätta en hög nivå av dataskydd.

Därför måste kommunens nämnder och kommunens bolag skydda informationen så:

- att den alltid finns när den behövs (tillgänglighet)
- att den går att lita på, att den är korrekt och inte heller manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)
- att det går att koppla åtkomst till en identifierad användare och tidpunkt (spårbarhet)

Skyddet måste anpassas efter behovet och handlar om att hantera de risker som kan medföra att kommunens nämnder och av kommunen majoritetsägda bolag inte kan genomföra sitt uppdrag. Detta kan i sin tur leda till att skada uppstår på skyddsvärden som människors liv och hälsa, samhällets funktion, demokrati, rättssäkerhet och mänskliga fri- och rättigheter, ekonomi och miljö samt nationell suveränitet

Syfte

Syftet med policyn är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet och dataskydd i Älvkarleby kommuns nämnder och i styrelser för av kommunen majoritetsägda bolag.

Inriktning och tillämpning

Älvkarleby kommuns inriktning är att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet (LIS). I detta arbete ska ISO/IEC 27001 och ISO/IEC 27002 utgöra en grund. För att hålla rätt nivå och rätt inriktning ska kommunens informationssäkerhet utgå från riskanalyser inklusive informationsklassningar på olika nivåer i organisationen.

Informationshantering ska skyddas på ett kostnadseffektivt sätt där risk vägs mot nytta på ett dokumenterat och kommunicerbart sätt. Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet.

Ledningssystemets regler gäller all information som hanteras av verksamheten och alla medarbetare som utför kommunens uppdrag. Som medarbetare räknas även extern anlitade aktörer så som konsulter inom ordinarie verksamhet. Reglerna ska tillämpas då kommunen upphandlar produkter och tjänster som kan påverka informationssäkerheten.

Avgränsning

Ledningssystemet omfattar inte de krav som följer av säkerhetsskyddslagen

Definition och begrepp

Informationssäkerhet – Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.

Informationsägare – Den som har ansvar för att information förvaltas, behandlas och kommuniceras på ett säkert sätt i sin egen verksamhet. Informationsägaransvaret är en del av chefsansvaret. Medarbetarna i en verksamhet utför det operativa arbetet med informationssäkerhet, men de innehar inget informationsägaransvar.

Informationssäkerhetssamordnare – Den eller dem som arbetar strategiskt och stödjande med informationssäkerhet eller dataskydd inom kommunstyrelsens förvaltning. Dess främsta uppgift är att stödja nämndernas och bolagens verksamheter inom sitt särskilda expertområde samt skapa långsiktiga planer för informationssäkerhet- och dataskyddsarbetet.

Behandling (av personuppgifter) - Behandling är ett vidsträckt begrepp och innefattar allt som kan göras med personuppgifter. Till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring av personuppgifter.

Känsliga personuppgifter - Personuppgifter som till exempel avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Personuppgiftsansvarig - Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Det är alltså är inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Även en fysisk person kan vara personuppgiftsansvarig vilket till exempel är fallet för enskilda firmor.

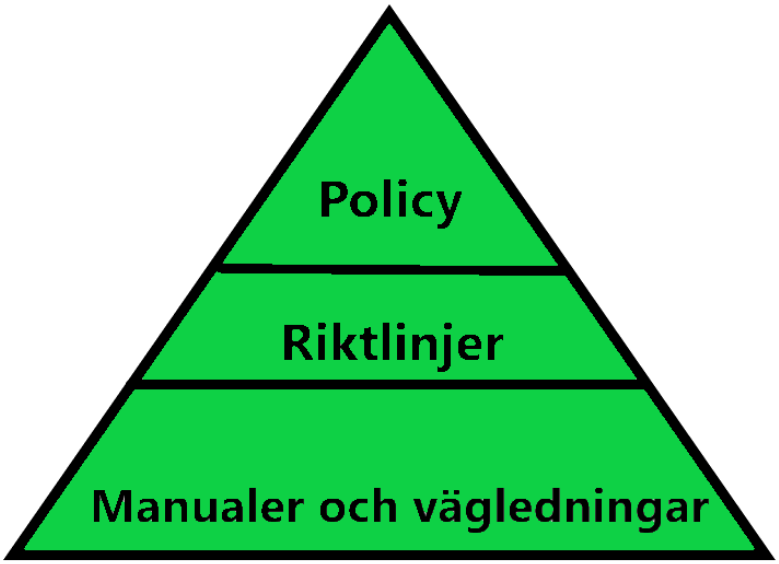
Personuppgiftsbiträde - Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Personuppgiftsincident - En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter.

Tredje land - En stat som inte ingår i EU eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Älvkarleby kommuns ledningssystem för informationssäkerhet (ÄLIS)

Älvkarleby kommuns ledningssystem styr informationshanteringen så att informationen hanteras med den säkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Styrningen omfattar att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.



Ledningssystemet ska dokumenteras i denna policy samt i riktlinjer och rutiner ordnade i en hierarkisk struktur. Ledningssystemets dokumentation ska ses som en helhet och det ska finnas en spårbarhet mellan olika ingående dokument. Ledningssystemets viktigaste del är dock inte dokumentation utan medarbetarnas kunskap, medvetenhet och motivation. Dialog och samverkansytor inom dataskydds- och informationssäkerhetsfrågor samt målgruppsanpassat material är därför centrala funktioner i ledningssystemet. Det ska finnas ett dataskydds- och informationssäkerhetsråd med representation från kommunens förvaltningar, av kommunen majoritetsägda bolag och specialistfunktioner inom kommunstyrelsen. Forumet sammankallas regelbundet och leds av informationssäkerhetsansvarig.

Mål för ledningssystemet

- Informationssäkerhetsarbetet ska stärka kommunens nämnders och bolags förmåga att identifiera hot, sårbarheter och risker avseende de egna informationstillgångarna samt skapa förutsättningar att reducera dessa risker till en acceptabel nivå.

- Det ska finnas ett tydligt ansvar för kommunens informationshantering och de resurser som används för att stödja den.
- Varje förvaltning- och bolagsledning ska bedöma vilka risker som är acceptabla och vilka som måste åtgärdas och förmedla detta via det generella chefsansvaret.
- Informationssäkerhet ska utgå från verksamhetens behov och uppdrag. Informationssäkerhetens nytta för verksamheten ska tydliggöras genom bland annat process- och informationskartläggning. Ansvaret för informationssäkerhet ska vara känt och accepterat inom verksamheterna.
- Externa krav på dataskydd och digital infrastruktur som i sin tur ställer krav på informationssäkerhetsåtgärder ska vara integrerade i det generella informationssäkerhetsarbetet.
- Informationssäkerhet ska vara utformat så att det tar hänsyn till de starkt skiftande krav som kan finnas inom kommunens olika verksamheter.
- Det ska finnas en beslutad metod för informationsklassning som även innehåller standardiserade skyddsnivåer.
- Centrala säkerhetsåtgärder som informationsklassning, styrning av åtkomst, loggning, incident- och kontinuitetshantering ska vara prioriterade i informationssäkerhetsarbetet.
- Kommunen ska ha tillgång till tillräcklig kompetens inom informationssäkerhetsområdet för att kunna hantera den komplexa kravbilden. Kompetensen ska finnas både i form av spetskompetens och i form av en bred förståelse av betydelsen av informationssäkerhet hos medarbetarna.
- Det ska finnas en säkerhetskultur som uppmuntrar engagemang hos alla medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten.

Ansvar och roller

Ansvaret för informationssäkerhet delas upp i ett ledningsansvar och ett verksamhetsansvar.

Ledningsansvar

Kommunstyrelsen har det yttersta strategiska ansvaret för informationssäkerhetsarbetet inom Älvkarleby kommun. Kommundirektören har ansvar för att genomföra de intentioner som formuleras i denna policy i kommunstyrelsens verksamhet. I detta ansvar ingår också att säkerställa att det finns styrdokument för LIS och resurser för att genomföra det som dessa styrdokument föreskriver. Kommundirektören ska ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och besluta om hur dessa risker ska hanteras. Arbetet med lägesbilden ska när så är lämpligt samordnas med kommunens övriga riskhantering.

Informationssäkerhetsansvarig ska, i enlighet med kommundirektörens beslut strategiskt och stödjande driva informationssäkerhetsarbetet framåt. Informationssäkerhetsansvarig ska som stöd för kommunens verksamhetsplanering årligen ta fram ett förslag på plan för informationssäkerhetsarbetet. I rollen ingår även att leda ett dataskydds- och

informationssäkerhetsråd med representation från kommunens förvaltningar och majoritetsägda bolag.

Verksamhetsansvar

Att utveckla och upprätthålla informationssäkerhet enligt LIS är en del i kommunens generella chefsansvar. Förvaltningschef har det övergripande ansvaret för informationssäkerheten inom respektive förvaltning, även kallat informationsägaransvar. Detta innebär ansvar för tillämpningen av ledningssystemets regelverk i den egna förvaltningen. Detta ansvar innebär även bland annat att se till att personalen hanterar information enligt gällande styrdokument samt anpassning av LIS-regler för den egna verksamheten. Respektive avdelningschef har ansvar för att utnämna representanter till dataskydds- och informationssäkerhetsråd. VD för kommunens majoritetsägda bolag har samma ansvar som en förvaltningschef.

Ansvarsfördelningen mellan IT-nämnden och Älvkarleby kommun gällande IT-säkerhet och informationssäkerhet regleras i IT-nämndens reglemente. IT-nämndens förvaltning har ansvar för att omsätta LIS funktionella krav på säkerhet till tekniska lösningar, när det faller inom deras ansvarsområde enligt deras reglemente. Älvkarleby kommun ansvarar för säkerheten i de tekniska lösningar som faller inom kommunens ansvar enligt IT-nämndens reglemente.

Dataskydd och personuppgiftshantering

Denna informationssäkerhets- och dataskyddspolicy fastställer övergripande mål och intentioner för arbetet med hantering av personuppgiftsbehandling. Behandling av personuppgifter innefattar all systematisk, automatiserad och digital hantering av personuppgifter.

Älvkarleby kommuns hantering av personuppgifter ska ske endast då det finns en laglig grund för att göra detta och då på ett så begränsat sätt som möjligt. Personuppgifter som ska hanteras ska vara korrekta och det ska vara lätt för utomstående att få insyn i hur hanteringen sker.

Varje nämnd och bolagsstyrelse är personuppgiftsansvarig för den egna verksamheten. Ett fortlöpande dokument som beskriver vilka personuppgiftsbehandlingar som sker i verksamheterna, kallat registerförteckning, ska upprättas av varje nämnd och bolagsstyrelse.

När personuppgiftsansvarig (PUA), det vill säga nämnd eller styrelsen för ett av kommunen majoritetsägt bolag, låter en utomstående aktör behandla kommunens personuppgifter för kommunens räkning skapas en personuppgiftsbiträdesrelation. För att reglera hanteringen och behandlingen av personuppgifter mellan personuppgiftsansvarig och personupppgiftsbiträdet (PUB), ska ett personuppgiftsbiträdesavtal (PUB-avtal) alltid tecknas i samband med avtal. Alla tjänster, produkter eller licensierade program som behandlar personuppgifter som kommunen inom sina myndighetsuppdrag samlat in och

förvaltar, och som hanteras av aktörer utanför kommunen för kommunens räkning, bör regleras via ett PUB-avtal.

Verksamhetschef, förvaltningschef eller VD som vid kommunal förvaltning eller av kommunen majoritetsägt bolag tecknar avtal för nämnden eller bolagsstyrelsens räkning ansvarar för att också ett PUB-avtal tecknas. Det är upp till varje nämnd och av kommunen majoritetsägt bolagsstyrelse att bestämma om beslut att ingå PUB-avtal tas av verksamhetschef, förvaltningschef eller av nämnden/bolagsstyrelsen själv.

Personuppgiftshantering i Älvkarleby kommun

Personuppgifter ska behandlas med utgångspunkt i att

- All behandling ska ske i enlighet med gällande lagstiftning
- De endast behandlas för berättigat ändamål som är fastställt innan behandlingen påbörjas
- De är korrekta och uppdaterade
- Risker för skada för den registrerade minimeras genom aktiv riskhantering och lämpliga skyddsåtgärder
- Endast behöriga ska få åtkomst
- De ska skyddas så de inte förstörs oavsiktligt
- De bevaras i identifierbar form så länge det är nödvändigt för ändamålet
- Tillämpa inbyggt dataskydd och dataskydd som standard genom att ta hänsyn till integritetsfrågor och bygga in lämpliga säkerhetsmekanismer i lösningar
- att överföring till tredje land inte sker utan adekvata säkerhetsåtgärder
- den registrerade kan ta del av de uppgifter som kommunen hanterar och lagrar om hen, rätta felaktiga uppgifter och, om det inte strider mot kommunens myndighetsutövning eller andra grundläggande intressen, få uppgifter raderade.

Insamlade uppgifter kommer endast att hanteras för det ändamål som uppgivits och lagras endast så lång tid som ändamålet motiverar. Enda undantag från detta är ytterligare behandling för arkivändamål som motiveras av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Organisation av arbetet med personuppgiftshantering

Kommunstyrelsen beslutar övergripande om viljeinriktning för personuppgiftsarbetet. Varje nämnd och bolagsstyrelse är personuppgiftsansvarig för sina egna personuppgiftsbehandlingar. Detta innebär att bolagsstyrelser och nämnder är ytterst ansvariga för att:

- följa gällande lagstiftning
- fastställa ändamål med behandlingar
- säkerställa att det finns ett eller flera Dataskyddsombud
- ansvara för att noggrann dokumentation av behandlingar finns
- säkerställa att det görs konsekvensbedömningar om behandlingar sannolikt medför en hög risk för den registrerades integritet

- säkerställa att personuppgiftsincidenter rapporteras till tillsynsmyndigheten
- tillgodose registrerades rättigheter gällande information, tillgång (utlämning), rättning, begränsning, invändning och dataportabilitet

Dataskyddsombudets roll

Varje nämnd och styrelse för av kommunen majoritetsägt bolag har ansvar för att utse ett eller flera Dataskyddsombud som granskar dess hantering av personuppgifter. Kommunens och bolagens Dataskyddsombud ska fortlöpande kontrollera att dataskyddet fungerar enligt ovanstående och, om så inte sker, rapportera till personuppgiftsansvariga. Dataskyddsombud är en oberoende funktion som ska anmälas till tillsynsmyndigheten. Dataskyddsombudet kan ha andra roller om det inte leder till en intressekonflikt. Uppgifterna för Dataskyddsombudet omfattar bland annat att:

- informera och ge råd till personuppgiftsansvarig
- övervaka efterlevnad av dataskyddsförordningen vid personuppgiftsbehandlingar
- ge råd vid riskanalyser och vara ett stöd vid konsekvensbedömningar
- vara kontakt för registrerade och tillsynsmyndighet
- samarbeta och begära förhandsråd av tillsynsmyndighet vid behov

Personuppgiftsansvarig ska bland annat säkerställa att dataskyddsombudet inte tar emot instruktioner eller blir föremål för sanktioner för att ha utfört sina uppgifter och på ett korrekt sätt och i god tid deltar i de större eller mer komplicerade frågor som rör skyddet av personuppgifter.

Dataskyddsombudet ska rapportera direkt till högsta förvaltningsnivå.

Uppföljning

Uppföljning av kommunens arbete med informationssäkerhets- och dataskyddsarbete ska ske på ett regelbundet och strukturerat sätt samt utföras genom interna kontroller och revisioner av oberoende part.