



Riktlinjer för informationssäkerhet

Dnr KS 2024/219

Beslutat av: Kommunstyrelsen

Datum reviderad: 2025-11-26

Dokumentet gäller för: Samtliga nämnder
och bolag

Dokumentansvarig: Kansliavdelningen

Giltig till: Tillsvidare

Revideras: Aktualitetsprövas en gång per
mandatperiod

Innehåll

.....	1
INLEDNING	3
UNDANTAG	3
SYFTE	3
OM INFORMATIONSSÄKERHET	4
KONFIDENTIALITET/SEKRETESS	4
RIKTIGHET	4
TILLGÄNGLIGHET	4
SPÄRBARHET	4
ÅTGÄRDER.....	5
NIS2 / CYBERSÄKERHETSLAGEN	5
ROLLER OCH ANSVAR.....	5
HANTERING AV INFORMATIONSTILLGÅNGAR OCH ÅTKOMST TILL INFORMATION	5
VID ANSTÄLLNING	6
UNDER ANSTÄLLNING	6
VID AVSLUT AV ANSTÄLLNING.....	6
HANTERING AV IT-UTRUSTNING.....	6
ÅTKOMST TILL INFORMATIONSTILLGÅNGAR OCH IT-SYSTEM.....	7
KONTINUITETSHANTERING	7
RISKBEDÖMNING OCH RISKHANTERING	7
LEVERANTÖR OCH AVTAL	7
RUTINER FÖR HÄNDELSER/INCIDENTHANTERING INCIDENTRAPPORTERING.....	8
DISTANSARBETE	8
LÖSENORD PÅ ANVÄNDARKONTON I IT-SYSTEM.....	9
SKADLIG KOD OCH NÄTFISKE.....	9
UPPFÖLJNING	9
UTBILDNING OCH FORTBILDNING.....	9
INFORMATIONSKLASSNING	10

Inledning

Dessa riktlinjer konkretiserar informationssäkerhetspolicyn med mer detaljerad information, ska-krav och regler för hur information får hanteras inom kommunen. Det övergripande målet med riktlinjen är att tillse att det operativa informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning.

Riktlinjerna innehåller information och regler gällande säkerhet vid hantering av information inom Åstorps kommun och gäller för samtliga verksamheter inom kommunen. Riktlinjerna ska ses som ett krav för hantering av information inom kommunen och ska fungera som ett praktiskt stöd i arbetet med informationssäkerhet.

Utgångspunkten för Åstorps kommuns informationssäkerhetsarbete är att följa den etablerade standarden inom området, GDPR, lagen om cybersäkerhet och internationella standarder som ISO 27001 och övriga tillämpliga lagar inom dataskydd. Detta stämmer väl överens med Myndigheten för samhällsskydd och beredskaps (MSB) rekommendation om hur informationssäkerhetsarbetet ska bedrivas inom offentlig förvaltning.

Denna riktlinje gäller för alla anställda, förtroendevalda, leverantörer och externa parter som hanterar eller har tillgång till kommunens informationssystem eller data. Riktlinjen omfattar all hantering av information, oavsett om den sker elektroniskt, manuellt eller i annan form. Riktlinjen fastställer ska-krav.

Undantag

Den verksamhet och informationshantering som träffas av säkerhetsskyddslagen omfattas inte av kraven i denna riktlinje. För sådan hantering gäller Säkerhetsskyddslagen.

För verksamheter som bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen gäller inte skyldigheten att lämna uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (1 kap 13 § cybersäkerhetslagen). Den del av verksamheten som omfattas av säkerhetsskydd undantas dessutom från skyldigheterna i 2 kap. 3–10 §§ cybersäkerhetslagen (1 kap. 12 § CSL).

Syfte

Syftet med riktlinjerna är att konkretisera informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen. Det ska finnas ytterligare instruktioner där det framgår vad/hur man ska göra för att uppfylla kraven i sin roll.

Om informationssäkerhet

Informationssäkerhet innebär att skapa och upprätthålla ändamålsenligt skydd för all typ av information. Detta inkluderar alla former av information, såsom text, ljud, bilder och film, oavsett hur informationen lagras, bearbetas eller kommuniceras. Skyddet kan ske med hjälp av digitala verktyg, papper eller genom direkt mänsklig kommunikation som tal. Medan IT-säkerhet fokuserar på att skydda information inom IT-system, omfattar informationssäkerhet all information, oavsett dess form. Det inkluderar inte bara information i IT-system utan även pappersbaserad information och information som finns i våra huvuden.

Informationssäkerhet är ett teknikneutralt begrepp som innebär skydd av information, oavsett om den är muntlig, pappersbunden eller digital. Syftet med informationssäkerhet är att säkerställa att rätt information är tillgänglig för rätt mottagare vid rätt tidpunkt.

Skyddet syftar till att upprätthålla informationens:

Konfidentialitet/sekretess

Konfidentialitet ska ses i ett bredare perspektiv och inkluderar både personlig integritet och sekretess enligt offentlighets- och sekretesslagen. Det innefattar även andra krav på att information inte ska bli tillgänglig för obehöriga.

Riktighet

Riktighet innebär att informationen som hanteras ska vara oförvanskad och skyddad från otillåten manipulering. Enligt dataskyddsförordningens princip om riktighet ska informationen dessutom vara tillförlitlig och korrekt. Detta innebär bland annat att rätt uppgifter hämtas från rätt datakälla för avsett syfte, och att felaktiga uppgifter rättas vid behov.

Tillgänglighet

Tillgänglighet innebär inte bara att informationen ska vara tillgänglig vid en given tidpunkt, utan även över tid, i enlighet med bevarande- och gallringsplaner enligt arkivbestämmelser.

Spårbarhet

Att i efterhand kunna följa specifika aktiviteter eller händelser till ett identifierat objekt eller användare.

Åtgärder

Informationssäkerhet inkluderar ett brett spektrum av åtgärder och tekniker, såsom:

Åtgärd	Beskrivning
Åtkomstkontroll	Begränsning av vem som får tillgång till olika typer av information.
Kryptering	Omvandling av information till en form som endast kan läsas av behöriga användare.
Säkerhetskopiering	Skydd av data genom regelbunden säkerhetskopiering för att kunna återställa förlorad information.
Incidenthantering	Processer för att identifiera, rapportera och hantera säkerhetsincidenter, som dataintrång eller systemfel.
Utbildning och medvetenhet	Träning av anställda för att förstå säkerhetsrisker och hur man skyddar organisationens information.

Att skydda information effektivt innebär inte bara tekniska åtgärder utan även organisatoriska och administrativa processer, i linje med standarder som ISO 27001.

NIS2 / Cybersäkerhetslagen

Kommunens informationssäkerhetsarbete ska följa de krav som ställs i cybersäkerhetslagen, vilken bygger på EU:s NIS2-direktiv. Lagen innebär att kommuner omfattas av tydligare krav på riskhantering, incidentrapportering och säkerhetsåtgärder för att skydda samhällsviktig verksamhet.

Det praktiska arbetet med att anpassa kommunen till cybersäkerhetslagen sker inom ramen för kommunens ledningssystem för informationssäkerhet (LIS).

Roller och ansvar

Roller och ansvar definieras och tilldelas i den av Åstorps kommuns kommunfullmäktige antagna informationssäkerhetspolicy.

Den primära målgruppen för detta dokument är alla medarbetare, objektägare (informationsägare, systemägare), IT-verksamhet och informationssäkerhetsorganisationen.

Hantering av informationstillgångar och åtkomst till information

Åstorps kommun hanterar stora mängder information som har ett högt skyddsvärde. Det är exempelvis säkerhetsskyddsklassad information, upphandlingar, utredningar inom socialtjänst och annan känslig information.

Viktiga informationstillgångar ska identifieras och klassificeras för att möjliggöra en lämplig skyddsnivå med utgångspunkt i att obehöriga inte kan få tillgång till informationen (*konfidentialitet*), att informationen finns tillgänglig när den behövs (*tillgänglighet*), att den är korrekt (*riktighet*) samt att den går att spåra över tid (*spårbarhet*).

Viktiga informationstillgångar ska tilldelas en informationsägare som fattar beslut om krav på skydd av informationstillgången.

All tillgång till information inom Åstorps kommun ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga får tillgång till informationen.

Behörigheter till information och system ska baseras på aktuella arbetsuppgifter och organisatorisk tillhörighet och ska därtill följas upp minst två gånger per år. Varje användares identitet ska kunna verifieras och alltid vara spårbar till en fysisk person.

För att kunna säkerställa korrekt användning av behörigheter behöver i vissa fall loggning och uppföljning genomföras. Informationsägaren beslutar om vilka säkerhetsåtgärder som krävs för åtkomst till information baserat på genomförd informationsklassificering och riskbedömning.

Vid anställning

Innan informationstillgångar överlämnas till behörig ska mottagaren informeras om informationens skyddsvärde avseende konfidentialitet, tillgänglighet, spårbarhet samt riktighet.

Under anställning

Vid anställning och löpande under anställningen ska medarbetare informeras om sitt ansvar för informationssäkerhet samt gällande lagkrav, exempelvis avseende allmänna handlingar och sekretess.

Medarbetare ska också upplysas om att bristande efterlevnad av dessa regler kan utgöra lagbrott och bryta mot anställningsavtalet, vilket i allvarliga fall kan leda till uppsägning eller avsked.

När anställda hanterar sekretessbelagd information ska de påminnas om gällande sekretessregler och de skyldigheter som följer av lag.

Sekretessen gäller inte enbart anställda i Åstorps kommun. Vid anlitan av konsulter eller andra externa uppdragstagare ska det tydliggöras om de deltar i verksamheten på samma villkor som kommunens anställda.

Vid avslut av anställning

Nämnder och bolag ska i rutin för avslut av anställning inkludera informationssäkerhetsperspektivet som säkrar återlämnande av informationstillgångar samt medvetenhet om fortsatt tystnadsplikt.

Hantering av it-utrustning

Nämnder och bolag ansvarar för att det finns uppdaterad inventarieförteckning över all it-utrustning. Det gäller intern, men även extern utrustning såsom surfplattor till förtroendevalda eller datorer till skolelever.

Åtkomst till informationstillgångar och it-system

Behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och organisatoriska tillhörighet för att endast ge åtkomst till de informationstillgångar som behövs för att lösa arbetet.

Endast informations- eller systemägare får ge konsulter tillgång till it-system och detta ska dokumenteras och regelbundet följas upp.

När en anställd har avslutat sin anställning, eller en konsult har avslutat ett konsultuppdrag, ska åtkomst till informationstillgångar tas bort.

Kontinuitetshantering

Det är viktigt att fastställa hur länge avbrott är acceptabla. För att hitta rätt ambitionsnivå ska juridiska krav samt verksamhetens behov av tillgång till information dokumenteras och riskbedömning genomföras. Kontinuitetsplanerna ska innefatta reservrutiner och övriga åtgärder som kan vidtas för att säkerställa verksamhetens kontinuitet.

Om Åstorps kommun är beroende av en annan organisation som till exempel en leverantör ska även leverantören vara involverad i arbetet. Varje avdelning behöver utforma, införa och upprätthålla processer, rutiner och säkerhetsåtgärder för att säkerställa den nivå av kontinuitet för informationssäkerhet som krävs vid en svår situation, exempelvis under en kris eller katastrof.

Riskbedömning och riskhantering

Nämnder och bolag ansvarar för att analyser genomförs för verksamheter samt it-system avseende vilka risker som kan påverka deras informationstillgångar. Med utgångspunkt i denna bedömning ska beslutas hur riskerna ska hanteras och nödvändiga åtgärder ska vidtas för att upprätthålla rätt skyddsnivå för informationen.

Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras när förutsättningarna väsentligen förändras, t.ex. vid köp av ett nytt system, organisationsförändringar eller förändrat arbetssätt.

Varje nämnd och bolag ska minst årligen genomföra en riskanalys för att identifiera de största riskerna mot de informationstillgångar som hanteras. Denna analys ska dokumenteras och redovisas för nämnden.

Leverantör och avtal

Innan anskaffning av ett system som ska hantera information ska analys ske av vilka krav avseende informationssäkerhet ska ställas.

Avtalet ska specificera hur händelser som rör informationssäkerhet ska hanteras då de uppstår hos leverantören relaterat till de informationstillgångar de hanterar åt nämnden eller bolaget.

Avtalet ska specificera vad som händer om leverantören inte följer de krav som ställts gällande informationssäkerhet.

Nämnder och bolag ansvarar för att uppföljning sker gällande hur leverantörer de har avtal med hanterar informationssäkerheten.

Incidentrapportering

Alla medarbetare ska omedelbart rapportera incidenter som kan påverka informationssäkerheten.

IT-relaterade incidenter hanteras enligt EttIT:s it-anvisningar, medan informationssäkerhetsincidenter hanteras enligt kommunens rutin för incidenthantering, varav båda finns på kommunens intranät.

Då nämnder och bolag rapporterar incidenter rörande brister i informationssäkerheten till tillsynsmyndigheter i enlighet med lag ska kommunstyrelsen, eller funktion med uppdrag därifrån, informeras om detta.

Distansarbete

Vid distansarbete gäller samma krav på informationssäkerhet som vid arbete på huvudarbetsplatsen. Det innebär att information ska skyddas mot obehörig åtkomst, oavsett var arbetet utförs.

Åtkomst till Åstorps kommuns nätverk får endast ske genom den krypterade fjärranslutning (VPN) som tillhandahålls av IT-avdelningen. Det är inte tillåtet att försöka nå kommunens IT-resurser på annat sätt.

Vid distansarbete gäller följande:

- Datorn ska placeras så att ingen obehörig kan se information på skärmen eller höra samtal.
- Arbete med känslig eller sekretessbelagd information ska inte ske i publika miljöer.
- Datorn ska alltid låsas när den lämnas utan uppsikt, även för kortare stunder.
- Vid arbete i gemensamma utrymmen ska datorn placeras så att andra inte kan ta del av material på skärmen.
- Användaren ansvarar för att datorn inte lämnas obevakad och för att den förvaras på ett säkert sätt vid resor eller i offentliga miljöer.

Offentlighetsprincipen jämte sekretesslagen gäller även för distansarbete. Hantering av allmänna handlingar vid distansarbete ska ske med samma kvalitet och säkerhet som hanteringen vid huvudarbetsplatsen.

Vid incidenter där information kan ha kommit i orätta händer, felaktigt raderats eller förvanskats ska närmaste chef omgående informeras.

För detaljerade tekniska krav hänvisas till EttIT:s IT-anvisning för användare ”*Distansarbete*”.

Lösenord på användarkonton i it-system

Medarbetarna behöver säkerställa att användarkonton har starka lösenord vid inloggning eftersom lösenord är den främsta åtgärden som förhindrar att obehöriga får tillgång till information och användarkonton. Här gäller det att inte använda uppgifter såsom namn och favorithobby eller vanligt förekommande ord som kan kopplas till användaren.

Skadlig kod och nätfiske

Skadlig kod eller röjande av känslig information kan uppstå när en användare öppnar ett e-postmeddelande, importerar filer eller klickar på en felaktig länk. Vid så kallat nätfiske uppmanas användaren att klicka på en länk som ser trovärdig ut genom att efterlikna en legitim webbadress med små, svårupptäckta förändringar. Detta kan leda användaren till en falsk webbplats där bedragare kan samla in information eller få användaren att ladda ner filer som äventyrar säkerheten i kommunens IT-system.

Medarbetare i kommunen behöver vara observanta på detta och aldrig fylla i sådana uppgifter. Vid misstanke om nätfiske eller att man blivit utsatt ska närmaste chef omgående informeras.

Uppföljning

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten inom Åstorps kommun och därmed för uppföljning av denna.

Varje nämnd och bolag ska en gång per mandatperiod genomföra en revision av sin informationssäkerhet och göra en analys av hur skyddsåtgärder förhåller sig till gällande styrande regelverk samt aktuell hotbild. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas, anpassas och kompletteras. Nämnden och bolaget ska också avsätta resurser för att möta de hot som kan uppstå i den egna verksamheten.

Varje år ska nämnder och bolag följa upp status på informationssäkerheten inom det egna ansvarsområdet. Detta kan ske genom att tillse att interna och externa krav på verksamhetens informationshantering följs genom intern kontroll.

För att säkerställa att styrande dokument efterföljs ska uppföljningar genomföras såväl årligen som när det inträffar väsentliga händelser som påverkar informationssäkerheten.

Utbildning och fortbildning

Informationssäkerhet omfattar alla medarbetare i Åstorps kommun. I det kontinuerliga arbetet med att uppnå och säkerställa informationssäkerhet samt stärka säkerhetskulturen är medarbetarens kunskap av yttersta väsentlighet. Nämnder och bolag ansvarar för att medarbetare får den utbildning i informationssäkerhet som behövs för att säkerställa säker hantering av de informationstillgångar som medarbetaren kan komma att ta del av.

Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Det är även nämndens och bolagets ansvar att säkerställa att lämplig kunskapsnivå bibehålls under medarbetarens hela anställningstid.

MSB:s utbildning [Digital informationssäkerhetsutbildning för alla \(Disa\)](#).

Informationsklassning

All information inom kommunen ska klassificeras för att tilldelas ett lämpligt skydd. Bedömning av skyddsbehov ska göras enligt kommunens modell för informationsklassning, som omfattar fem skyddsnivåer (nivå 0–4).

Nivåerna beskrivs djupare i dokumentet 'Instruktion för informationsklassning'. Skyddsbehovet bedöms utifrån informationssäkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Nivåbestämningen ska utgå från bedömd skada vid obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång.