ARJEPLOGS KOMMUN
ÁRJEPLUOVE KOMMUVNNA

Informationssäkerhetspolicy

Dokumenttyp	**Dokumentnamn**	**Fastställd/upprättad**	**Beslutsinstans**	**Giltighetstid**
Policy	Informationssäkerhetspolicy	Kommunfullmäktige 2024-12-09 § 100.	Kommunfullmäktige	Tillsvidare
Dokumentansvarig	**Version**	**Senast reviderad**	**Dokumentinformation**	
Kommunchef	1.0		Dnr 2024/676, 009	Detta dokument gäller för Politik och förvaltning

Innehåll

1. Inledning

Information är en viktig resurs för Arjeplogs kommun och är av stor betydelse för alla våra verksamheter. I Kommunen hanterar vi varje dag mängder av information som handlar om allt vi gör, t.ex. skola, vård och omsorg, stadsplanering, bygglov osv. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd till den informationen. Viss information är känslig och måste skyddas från obehöriga att ta del av, det kan exempelvis vara information vi måste skydda av hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada, eller handla om känslig information om samhällsviktig verksamhet som skulle kunna innebära ökad risk eller sårbarhet mot verksamheten om den hamnar i fel händer.

Informationssäkerhet begränsas inte till säkerhet i verksamhetssystem, utan omfattar information i alla dess former och oavsett hur informationen lagras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bild och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal. Informationssäkerhet omfattar alltså *all* information samt hur den hanteras, förvaras, kommuniceras och skyddas.

Det finns en hel del lagar och föreskrifter kommunen måste leva upp till, exempelvis offentlighet- och sekretesslagstiftningen samt dataskyddsförordningen. Men kommunen har även ett eget intresse av att skydda vår information, felaktig hantering av information kan påverka verksamhetens förmåga att utföra sin uppgift, det kan ha negativ påverkan på ekonomi, individ eller externa intressenter. Felaktig hantering av information kan även leda till juridiska konsekvenser samt förlorat förtroende/anseende.

1.1. Syfte och omfattning

Informationssäkerhetspolicyn är ett övergripande dokument som beskriver kommunens övergripande mål och inriktning kopplat till strategiskt informationssäkerhetsarbete samt hur ansvaret i dessa frågor är fördelat. Policyn syftar även till att konkretisera och tillse att det övergripande operativa informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning.

Syftet med ett strategiskt informationssäkerhetsarbete är att skydda organisationens information och innefattar bl.a. reglering av hur ansvaret ska fördelas samt hur kommunens anställda ska agera när det gäller skydd av information, såväl inom kommunen som i kontakt med externa parter. Den innefattar även reglering av hur det faktiska informationssäkerhetsarbetet ska genomföras i kommunens verksamheter gällande hantering av elektroniska data, fysisk information och muntlig kommunikation.

Kommunstyrelsen ska, med stöd av denna policy, kunna styra kommunens informationssäkerhetsarbete i enlighet med MSB[1]:s rekommendationer för kommunens informationssäkerhet samt med beaktande av kraven i informationssäkerhetsstandarden ISO 27000. Detta görs strategiskt, bland annat genom att ange vad som ska skyddas i kommunens verksamheter samt hur skyddet ska utformas.

Policyn gäller för både politik och förvaltning inom Arjeplogs kommun, och lämnar inget utrymme att besluta om lokala regler som avviker från dessa. Enskilda verksamheter kan dock vid behov ta fram egna kompletterade anvisningar och riktlinjer såvida de inte avviker från vad som är beslutat om i denna policy.

1.2. Ansvar och befogenheter

Kommunfullmäktige är beslutsfattande instans för informationssäkerhetspolicyn och beslutar således om vilken inriktning kommunen ska ha i det strategiska informationssäkerhetsarbetet.

Kommunstyrelsen ansvarar för det övergripande och strategiska arbetet med informationssäkerhet. Med detta menas bland annat att Kommunstyrelsen anger vad som ska skyddas, hur en verksamhet ska avgöra lämplig skyddsnivå samt hur det faktiska skyddet uppnås, detta kan exempelvis vara genom fastställda riktlinjer för det strategiska informationssäkerhetsarbetet.

Kommunchefen har ansvar för att det strategiska informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktige fastställda informationssäkerhetspolicyn.

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledning till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Det åligger varje verksamhetsansvarig att se till att sina medarbetare efterlever policy, riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås.

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd har även en skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Rapportering av brister och incidenter ska göras skyndsamt till närmsta chef samt i KIA.

Kommunens säkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, ex. IT-säkerhet eller andra relaterade frågor, fungerar som stöd till medarbetare, verksamheter och ledning.

[1] Myndigheten för samhällsskydd och beredskap. Byter namn till Myndigheten för civilt försvar från och med 1 januari 2025.

1.3. Mål

Målet med strategiskt informationssäkerhetsarbete handlar om att ha tydliga rutiner för hur information ska hanteras för att förhindra att information läcker ut, förvanskas eller förstörs. Det handlar även om att göra information lättillgänglig när den behövs och för rätt person.

1.3.1. Principer och arbetssätt för att uppnå mål

- Arbetet med informationssäkerhet ska vara systematiskt och långsiktigt.
- Informationssäkerhetsarbetet ska bedrivas i enlighet med de lagkrav som berör kommunens verksamheter.
- Det ska finnas en organisation för informationssäkerhetsarbetet med tydliga roller och ansvarsfördelningar.
- Chefer, medarbetare och förtroendevalda ska ha en grundläggande kompetens inom informationssäkerhet.
- Informationsklassning ska genomföras för all kommunens information för att kunna tilldelas lämpligt skydd.
- Kommunen ska fastställa krav på fysisk och teknisk säkerhet.
- Kommunen ska fastställa krav vid upphandling och i leverantörsavtal.
- Kommunen ska arbeta aktivt med att förhindra incidenter och att minimera risker när det kommer till hantering av information.
- Incidenter ska rapporteras, följas upp och åtgärdas.

2. Informationssäkerhet

2.1. Informationsklassning

Informationsklassning ska genomföras för all kommunens information för att därefter kunna tilldela informationen lämpligt skydd. Samtliga bedömningar av skyddsbehov för informationen ska göras enligt kommunens modell för informationsklassning (se rubrik 2.1.1. sid. 4). Bedömningar av skyddsbehov ska göras utifrån informationssäkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Konfidentialitet	Att känslig och sekretesskyddad information inte röjs för obehörig och att informationen kan åtkomstbegränsas
Riktighet	Att informationen ska vara tillförlitlig, korrekt och fullständig
Tillgänglighet	Att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
Spårbarhet	Att det är möjligt att säkerställa vem som har lagt till, ändrat eller raderat information

Olika typer av händelser och incidenter, som kan vara oavsiktliga eller avsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Information kan på ett oönskat sätt t.ex. stjälas, raderas, förändras eller göras otillgänglig.

En viss informationsmängd har krav på sig gällande de tre aspekterna som kan vara interna eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering. Dessutom har ofta externa aktörer behov och förväntningar som påverkar organisationens informationssäkerhet. Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbild, sårbarhet och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

2.1.1. Informationsklassningsmodell

Skyddsnivå	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
4 **Säkerhetsskydds-klassifierade uppgifter** Mycket högt skyddsbehov	Säkerhetsskydds-klassifierade uppgifter. Information som rör Sveriges säkerhet.	Information som om den inte är riktig och fullständig medför synnerligen allvarlig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför synnerligen allvarlig konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför synnerligen allvarlig konsekvens för kommunen eller annan part.
3 **Stark sekretess** Högt skyddsbehov	Information som innehåller uppgift som omfattas av stark eller absolut sekretess där felaktig spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.	Information som om den inte är riktig och fullständig medför allvarlig konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför allvarlig konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför allvarlig konsekvens för kommunen eller annan part.
2 **Sekretess** Förhöjt skyddsbehov	Information som omfattas av svag sekretess enligt OSL eller känsliga personuppgifter enligt GDPR, där felaktig spridning kan medföra betydande konsekvenser för kommunen eller annan part.	Information som om den inte är riktig och fullständig medför betydande konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför betydande konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför betydande konsekvens för kommunen eller annan part.
1 **Intern information** Grundläggande skyddsbehov	Information som är avsedd att spridas fritt enbart till medarbetare inom Arjeplogs kommun och till externa aktörer som behöver informationen.	Information som om den inte är riktig och fullständig medför måttligt negativ konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför måttligt negativ konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför måttligt negativ konsekvens för kommunen eller annan part.
0 **Öppen information** Inget skyddsbehov	Öppen information som är avsedd att spridas fritt inom och utom Arjeplogs kommun.	Information som om den inte är riktig och fullständig medför lindrig eller försumbar negativ konsekvens för kommunen eller annan part.	Information eller funktion som om den inte är tillgänglig medför lindrig eller försumbar negativ konsekvens för kommunen eller annan part.	Information eller aktivitet som om den inte är spårbar medför lindrig eller försumbar negativ konsekvens för kommunen eller annan part.

2.2. Medarbetarens ansvar för informationssäkerhet

Information behöver olika slags typ av skydd, det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, administrativt i form av regler eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp etc. Även medarbetarens kunskap och medvetenhet är ett nog så viktigt skydd, t.ex. att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information som t.ex. personuppgifter. Säkerhet är inte bättre än den svagaste länken, och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av Arjeplogs kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Arjeplogs kommun ställer krav på att samtliga medarbetare följer policy och fastställda riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare.

Vid underlåtenhet att följa policy och riktlinjer för informationssäkerhet följer Arjeplogs kommun regler enligt lagar och avtal. Lagbrott polisanmäls.

2.2.1. Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på kommunens information. Det kan t.ex. röra sig om:

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Personuppgiftsincidenter
- Brister i efterlevnad av denna informationssäkerhetspolicy

IT-relaterade incidenter ska snarast rapporteras till kommunens IT-avdelning, närmsta chef samt rapporteras i KIA. Medarbetare som upptäckt incidenter eller svagheter i IT-miljön ska inte själv försöka bevisa sådana, då detta kan försvåra framtida utredning samt riskerar ytterligare skada på IT-miljön. Övriga informationssäkerhetsincidenter ska i första hand anmälas till närmsta chef och rapporteras i KIA.

2.2.2. Föra register över behandling av personuppgifter

Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över sin behandling av personuppgifter. Dessa ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterade. På begäran ska registret kunna göras tillgängligt för IMY[2].

Registret[3] ska innehålla:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålet med behandlingen.
- En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket i dataskyddsförordningen, dokumentation av lämpliga skyddsåtgärder.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 i dataskyddsförordningen.

2.2.3. Användarbeteenden

Ett strategiskt informationssäkerhetsarbete är beroende av ett säkert användarbeteende, d.v.s. hur medarbetare hanterar informationen som är tillgänglig för dem. Användarbeteenden beror dels på vem vi är som person men även vilken kunskap och medvetenhet vi besitter, varför det är viktigt att komplettera med utbildning och information.

Arjeplogs kommun ska sträva efter en god kompetens och hög medvetenhet om hantering av information på ett säkert sätt inom verksamheten och för alla medarbetare. Det kan röra sig om allt från hur man hanterar sina lösenord, vad man diskuterar med kollegor eller anhöriga, hur man hanterar inkomna handlingar eller hur och med vad man väljer att arbeta med när man är på tjänsteresa.

Medarbetare inom Arjeplogs kommun ska ta ansvar för att delta på de utbildningsinsatser som erbjuds och kommuniceras ut internt för att stärka sin kompetens och medvetenhet inom säker informationshantering. Chefer ansvarar för att förmedla och följa upp deltagande vid arbetsplatsträffar.

[2] Integritetsskyddsmyndigheten.
[3] Enligt artikel 30 i Dataskyddsförordningen.

2.3. Åtkomstkontroll

Åtkomstkontroll av behörigheter är en viktig del för att kunna upprätthålla konfidentialitet, riktighet, tillgänglighet samt spårbarhet av information.

All personal inom Arjeplogs kommun ska ha de behörigheter som arbetsgivaren finner nödvändiga för att medarbetaren att kunna utföra sina arbetsuppgifter, det är närmsta chef som ansvarar för att medarbetaren får de behörigheter som krävs. I vissa fall kan en medarbetare behöva säkerhetsklassas om medarbetaren kommer vara i kontakt med och/eller hantera skyddsvärd information.

All personal har ansvar för att hantera sina behörigheter på ett säkert sätt, det kan handla om säker hantering av nycklar eller inpasserings-taggar/kort, säker hantering av lösenord eller koder samt att inte släppa in obehöriga i lokaler eller utrymmen eller ge tillgång till system de inte har tillgång till, obehöriga kan även innefatta andra medarbetare inom Arjeplogs kommun. Om en medarbetare behöver tillträde till ett system eller lokal/utrymme ska detta tas med närmsta chef.

3. Riskhantering och incidenthantering

Arjeplogs kommun ska arbeta aktivt med att förhindra incidenter och att minimera risker när det kommer till hantering av information. För ett effektivt arbete med god informationssäkerhet inom verksamheten krävs att risker, sårbarheter och incidenter identifieras, följs upp och åtgärdas.

Alla som är anställda inom Arjeplogs kommun har en skyldighet att rapportera identifierade risker, sårbarheter eller incidenter i KIA samt till närmsta chef, chef kan därefter vid behov ta det vidare till kommunens säkerhetssamordnare. Incidenter, risker eller sårbarheter kopplat till IT ska rapporteras till kommunens IT-avdelning. Vid händelse av att medarbetaren känner en otrygghet i att anmäla incidenten till närmsta chef finns möjlighet att rapportera incidenten direkt till säkerhetssamordnare eller kommunchef.

Det är av yttersta vikt att en rapportering sker oavsett hur liten eller stor bristen inom verksamheten är, oavsett om det är ett problem med rutiner, riktlinjer, system eller person.

3.1. Personuppgiftsincidenter

Personuppgiftsincidenter kan men behöver inte få konsekvenser för en enskild individ vid bristfällig hantering, men ska alltid rapporteras in som en personuppgiftsincident till närmsta chef om det kan innebära risk för den registrerade. Närmsta chef ska därefter rapportera händelsen till kommunens säkerhetssamordnare.

Personuppgiftsincidenter kan innebära risker för enskilda individers fri- och rättigheter och kan få allvarliga konsekvenser, till exempel:

- Ekonomisk skada
- Diskriminering
- Identitetsstöld
- Bedrägeri
- Skadlig ryktesspridning

Bristfällig hantering av registrerade personuppgifter kan vara:

- Personuppgifter som glömts framme eller hanteras oförsiktigt.
- Muntlig information som kan utgöra skada eller missaktning mot enskild individ.
- Digitalt eller analogt data som innehåller personuppgifter förloras eller stjäls.
- Någon ändrar personuppgifter utan tillstånd.
- Personuppgifter inte längre finns tillgängliga för den som behöver dem och leder till negativa konsekvenser för de registrerade.

3.2. IT-incidenter

Vid en IT-relaterad händelse ska du som medarbetare i första hand inte försöka lösa problemet själv då det kan skapa ytterligare skada på verksamhetens IT-struktur, vänd dig skyndsamt till IT för stöd och rådgivning och anmäl incidenten till närmsta chef om du misstänker att information har blivit röjd eller kan ha gått förlorad.

Exempel på IT-incidenter:

- Du misstänker att du blivit hackad eller fått in skadlig programvara på din dator.
- Du misstänker att ett program eller system du använder blivit hackat eller fått in skadlig programvara i programmet/systemet.
- Felaktig hantering av lösenord eller behörighet.

3.3. Sekretess- eller säkerhetsskyddsklassad information

Vid uppmärksammad eller misstänkt felaktig hantering av sekretessklassad information ska incidenten rapporteras till närmsta chef.

Det kan exempelvis vara:

- Sekretessklassad information inte hanterats på korrekt sätt.
- Digitalt eller analogt data som innehåller sekretessklassad information förloras eller stjäls.
- Obehörig har fått tillgång till sekretessklassad information.

Säkerhetsskyddsklassad information ska endast hanteras av personal med säkerhetsskyddsklassning, och berör således inte majoriteten av de anställda inom Arjeplogs kommun, även om samtliga anställda kan rapportera incidenter vid felaktig hantering. Vid uppmärksammad eller misstänkt felaktig hantering av säkerhetsskyddsklassad information (rikets säkerhet) ska detta rapporteras till kommunens säkerhetssamordnare eller kommunchef.

Det kan exempelvis vara:

- Säkerhetsskyddsklassad information inte hanteras på korrekt sätt, ex. lämnas framme för obehöriga att ta del av.
- Säkerhetsskyddsklassad information har röjts, förlorats eller blivit stulen.

3.4. Obehöriga i lokaler

Obehöriga ska inte ha obevakat tillträde till lokaler och utrymmen där skyddsvärd information finns tillgänglig. Om obehörig person uppmärksammas i sådana lokaler eller utrymmen ska personen avvisas från platsen och incidenten ska rapporteras i KIA samt till närmsta chef. Om personen kan misstänkas ha kommit över eller tagit del av skyddsvärd information ska detta framgå i incidentrapporteringen.

4. Externa parter och leverantörer

Externa parter och leverantörer ska inte få mer tillgång till information än de behöver för att utföra uppdraget, men krav ska ställas hur de som motpart ska hantera information som lämnas ut för att den inte ska röjas, förvanskas eller förstöras. Det är även viktigt att ha säkerställt hur leverantören ska använda informationen och hur de kommer kontrollera att kraven efterföljs inom deras verksamhet, med särskilt beaktande till information som kan anses skyddsvärd.

Om informationssäkerhetsåtgärder ska vidtas för att skydda känslig information som rör samhällsviktiga och digitala tjänster, men inte är av betydelse för Sveriges säkerhet, kan det bli aktuellt att beakta NIS-direktivet och den svenska nationella lagstiftning som omsätter NIS-direktivets bestämmelser. Dessa bestämmelser blir endast aktuella om det inte rör sig om säkerhetskänslig verksamhet enligt säkerhetsskyddslagstiftningen.

Om tjänsten kräver tillgång till säkerhetskänslig information ska Arjeplogs kommun göra en säkerhetsskyddad upphandling (SUA). Detta görs utifrån en analys av organisationens skyddsvärden, för att skydda verksamheter som är av betydelse för Sveriges säkerhet. Det är viktigt att ett säkerhetsskyddsavtal upprättas gentemot leverantören.

5. Tillsyn, efterlevnad och uppföljning

Informationssäkerhetspolicyn för Arjeplogs kommun ska vara ett vägledande styrdokument för hur kommunen ska uppfylla lagkrav och regler för att säkerställa en hälsosam kultur när det kommer till hantering av information.

5.1. Kommunstyrelsen

Kommunstyrelsen ansvarar för framtagande av att strategiska mål inom informationssäkerhetsarbetet antas och implementeras i organisationen.

5.2. Kommunchef

Ansvarar över att policyn efterlevs från chefer och följs upp inom organisationen, samt att arbetet med det strategiska informationssäkerhetsarbetet utvecklas, implementeras och följs upp.

5.3. Säkerhetssamordnare

Ansvarar för att policyn revideras samt ansvarar över tillsyn och kompetensutveckling inom informationssäkerhetsarbetet inom organisationen.

5.4. IT-chef

Ansvarar för att direktiv om IT-säkerhet och hur vi upprätthåller en god IT-infrastruktur förmedlas inom organisationen.

5.5. Chefer

Chefer agerar informationsansvarig inom sin verksamhet och ansvarar för att medarbetare inom deras verksamhet tar del av och efterlever policyn.

5.6. Medarbetare

Ansvarar över att ta del av policyn och efterleva den.

5.7. Fastighetschef

Fastighetschef har ett särskilt ansvar för kommunens fastigheter och skalskydd och ska skyndsamt informeras om eventuella brister kopplat till detta, då ett bristande skalskydd kan riskera skyddet av kommunens information.

———