Riktlinjer för informationssäkerhet

Riktlinjer för informationssäkerhet	
Fastställd:	Kommunstyrelsen 2024-06-11 § 91
Gäller från datum:	2024-06-12
Ansvarig:	Kommunchef
Diarienummer:	2024/321-167
Version:	1.0
Informationsklass:	Intern

Innehåll

Inledning

Sorsele kommuns informationssäkerhetspolicy är ett övergripande dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet. Detta dokument **Riktlinjer för informationssäkerhet** konkretiserar informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen.

Riktlinjernas omfattning

Dessa riktlinjer innehåller information och regler gällande säkerhet vid all hantering av information inom Sorsele kommun.

Riktlinjerna gäller för alla verksamheter i Sorsele kommun, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa.

I vissa fall kan ändå dessa riktlinjer gälla för kommunens bolag, liksom för andra externa aktörer, exempelvis när dessa använder sig av kommunens informationstillgångar, eller då det finns särskilda behov av samordning.

Riktlinjen beslutas initialt av kommunstyrelsen och därefter av kommunchef.

Struktur och läsanvisningar

Riktlinjer för informationssäkerhet är uppdelat i fyra kapitel (A-D) som riktar sig till olika målgrupper:

Kapitel		Innehåll	Primär målgrupp
A	Informationssäkerhet för medarbetare	Information och riktlinjer för hur information och IT ska hanteras i olika situationer.	Alla medarbetare
B	Styrning av informationssäkerhet	Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas.	Alla som arbetar med IT- och informationssäkerhet
C	Informationssäkerhet i verksamhetsnära förvaltning	Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t.ex. system och grupper av system.	Informationsägare, systemägare och verksamhetsledare
D	Informationssäkerhet i IT-miljön	Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT-säkerhet.	Chef och medarbetare på IT-enheten

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska. Samtliga riktlinjer är numrerade och i tabellform med rött huvud. Rader som innehåller riktlinjer för **konfidentiell** information och **höga skyddskrav** har dubbla linjer och nämnda termer är dessutom fetmarkerade. Exempel från Kapitel A om lagring i molntjänster:

Riktlinjer för lagring i molntjänster	
A.6.6	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
A.6.7	**Konfidentiell** information får inte lagras i molntjänster.

Andra tabeller, som inte innehåller riktlinjer, har tabellhuvuden i blå färg.

Kapitel A – Informationssäkerhet för medarbetare – har strukturerats för att stämma överens med avsnitten i utbildningen DISA (Datorstödd informationssäkerhetsutbildning för användare). DISA har skapats av Myndigheten för samhällsskydd och beredskap (MSB) och utgörs av ett antal filmer med vidhängande information. Tanken är man ska kunna genomgå DISA-utbildningen parallellt som man läser riktlinjerna i Kapitel A – Informationssäkerhet för medarbetare.

Informationsklassning är en central del i kommunens arbete med informationssäkerhet och finns med genomgående i riktlinjerna. Hur information klassas ska styra i vilken grad informationen ska skyddas. Sorsele kommuns modell för informationsklassning beskrivs i Kapitel B och information och regler för hur information ska klassas och skyddas utifrån denna återfinns i respektive kapitel.

Denna riktlinje är baserad på den svenska och internationella standarden ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder.

Dispenser och undantag

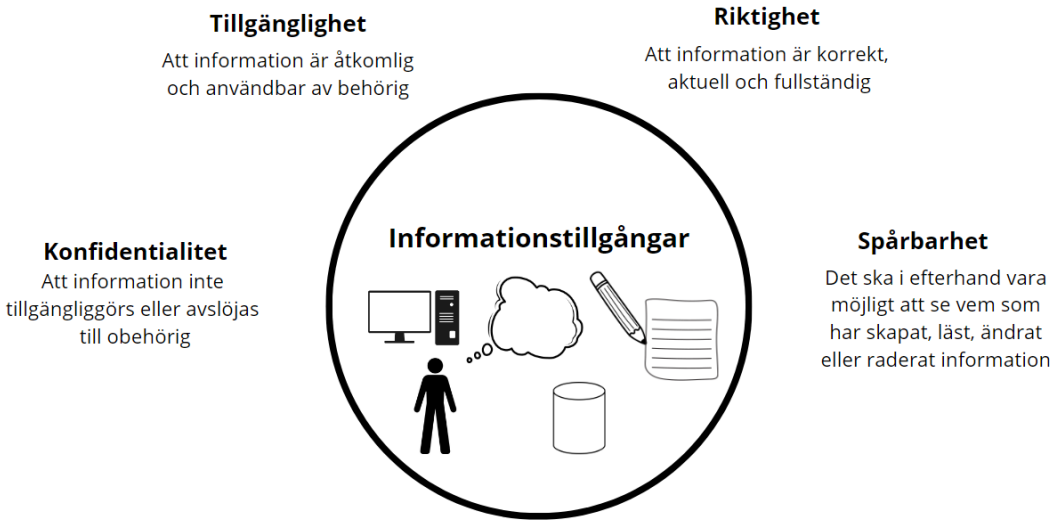
Ansökan om dispenser från dessa riktlinjer ska ställas till kommunchef. Sådana ärenden ska beredas med IT-enhet och säkerhetsansvarig för att underlätta beslut. Exempelvis kan en riskanalys ingå i beredningen av ärendet. Beslut om godkännande av undantag ska fattas av kommunchef i samråd med berörda.

Undantag från Riktlinjer för informationssäkerhet får aldrig vara permanenta utan ska ha en giltighetstid på som längst 2 år. Om behov av undantag kvarstår ska ärendet beredas på nytt och nytt beslut fattas om eventuellt godkännande.

Introduktion till informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former; text, ljud, bilder, film osv, och oavsett hur information lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, papper eller direkt av oss människor i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-baserad informationshantering handlar informationssäkerhet alltså om **all** information, oavsett form. Detta inkluderar förutom information i IT-system även pappersbaserad information och information som finns i våra huvuden.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet utgörs av de grundläggande aspekterna; att en informationstillgång ska vara konfidentiell, riktig, tillgänglig och spårbar (se Figur 1).



Figur 1: Informationssäkerhetens grundläggande aspekter

Olika typer av händelser eller incidenter, som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Därför är också spårbarheten en viktig aspekt. Information kan på ett oönskat sätt t.ex. stjälas, raderas, förändras eller göras otillgänglig.

En viss informationsmängd har krav på sig gällande de aspekterna som kan vara interna eller komma 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 som ofta innefattar krav på informationens konfidentialitet, riktighet och tillgänglighet. 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, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

Informationssäkerhet och digitaliseringen

Under det senaste decenniet har samhället genomgått en omvälvande förändring som ofta hänvisas till som den digitala transformationen. I dagens digitala era är användningen av datorer och internet inte bara en norm, utan en oumbärlig del av vardagen för privatpersoner, företag, myndigheter och andra organisationer.

Digitaliseringens möjligheter har expanderat avsevärt, och internetanvändningen har blivit ännu mer omfattande och diversifierad. Med en ständigt ökande anslutning till internet har privatpersoner möjlighet att utföra en mångfald digitala tjänster från hemmet, såsom bankärenden, inköp, deklaration, bokningar och omröstningar. Förväntningarna från samhället är nu höga, och det förväntas att myndigheter, företag och andra organisationer erbjuder digitala tjänster online.

Idag sträcker sig internetanslutningen långt bortom traditionella datorer; miljontals enheter, från kameror till bilar, är nu en del av Internet of Things (IoT). Samtidigt har artificiell intelligens (AI) blivit en integrerad del av vårt digitala landskap som möjliggör automatisering och analyser av stora datamängder.

Digitaliseringen betraktas som en katalysator och en drivkraft för en utveckling som skapar helt nya förutsättningar för samhället och dess invånare. Det är svårt att föreställa sig hur samhället kommer se ut om ytterligare tjugo år, men utvecklingen accelererar och öppnar upp möjligheter som vi bara har skrapat på ytan av.

Denna digitala omvandling har betydande konsekvenser för kommunal verksamhet. Nya koncept som e-hälsa, e-förvaltning, e-demokrati, intelligenta transportsystem och smarta städer integreras nu, och digitaliseringen sträcker sig långt bortom enbart kommunal IT-drift. Denna utveckling kommer att förändra fundamentala aspekter av hur vi agerar, hur processer genomförs och vilka möjligheter som blir tillgängliga. Informationen kommer att flöda i överväldigande volymer, genom och mellan olika organisationer samt till och från privatpersoner.

I dagens digitala era står vi inför både möjligheter och utmaningar som följer i digitaliseringens fotspår. Information är inte längre begränsad till enskilda organisationer, utan strömmar fritt mellan näringsliv, offentlig förvaltning, individer och över nationsgränser. Gränserna mellan ägande och ansvar för information suddas ut, vilket komplicerar definitionen av användningsvillkor och ansvarsfördelning, liksom lokaliseringen av ursprungsinformationen.

Internet, som nu fungerar som en arena för hela samhället, exponerar också dess baksidor. Virus, skadlig kod, bedrägerier, utpressning, stölder, näthat och stalking

manifesterar sig i olika former online. Organiserad kriminalitet, extremistgrupper, terrorister och stater har redan för länge sedan förflyttat delar av sina aktiviteter till den digitala världen. Det krävs inte längre expertkunskaper inom IT för att utföra destruktiva handlingar på nätet. Tjänster kan köpas på anonyma och krypterade marknadsplatser där skadlig verksamhet frodas. Sverige och internationellt drabbas regelbundet av informationsrelaterade incidenter, antingen till följd av avsiktliga attacker, misstag eller olyckor. Dessa trender utgör sammanlagt stora utmaningar för kommuners informationssäkerhet.

”Det övergripande målet med Sorsele kommuns digitaliseringsarbete är att förbättra kommunens tillgänglighet, service och effektivitet genom att utveckla verksamheternas arbetssätt, system och processer ur ett medborgar-, verksamhets och samhällsperspektiv.”

Information utgör en strategisk resurs för kommunen och genomsyrar alla dess verksamheter. I takt med att informationshantering och informationsflöden tar nya former i samhället och hotbilden förändras krävs ökad uppmärksamhet på informationssäkerhet för att Sorsele kommun ska kunna delta fullt ut i det digitala samhället. En fungerande informationssäkerhet möjliggör daglig verksamhet och användningen av ny teknik. Kortfattat en förutsättning för att kommunen ska fungera.

Termer och definitioner

Term	Definition
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Data	Representation av fakta i form av t.ex. tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Information	Innebörd i data, d.v.s. data tolkad av människor.
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information.
Informationssäkerhetspolicy	Organisationens viljeinriktning med informationssäkerhet uttryckt av dess ledning.
Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t.ex. rykte).
IT-resurs	IT-baserad komponent som hanterar information, t.ex. system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara.
IT-säkerhet	Säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet.
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas till obehörig.
Ledningssystem för informationssäkerhet (LIS)	Ett administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet.
Objekt	Ett objekt refererar kan referera till en informationsmängd eller ett system.
Riktighet	Att information är korrekt, aktuell och fullständig.
Sekretess	Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller har fått befattning om uppgiften.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs.
Tillgänglighet	Att information är åtkomlig och användbar av behörig.

Resurser och länkar

Informationssäkerhet för medarbetare

DinSäkerhet.se

En sida om risker och säkerhet för privatpersoner. DinSäkerhet drivs av MSB – Myndigheten för samhällsskydd och beredskap.

DinSäkerhet.se - Informationssäkerhet

Direktlänk till avsnittet om informationssäkerhet där det finns information om hur man skyddar sin information och IT-miljö i hemmet och privat.

DISA – Datorstödd informationssäkerhetsutbildning för användare

Den utbildning som tillhandahålls gratis av MSB och som anknyter till Kapitel A i dessa riktlinjer.

Krisinformation.se

Krisinformation.se är en webbplats som drivs av MSB och förmedlar information från myndigheter och andra ansvariga till allmänheten före, under och efter en stor händelse eller kris.

Stöldskyddsföreningen

Säkerhetsinformation m.m. för både privatpersoner och företag. Viss information finns om informationssäkerhet, bl.a. surfa säkert och ID-stölder.

Övriga kapitel

MSB

Myndigheten för samhällsskydd och beredskap, MSB, är en statlig myndighet med uppgift att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. MSB har i uppgift att samordna arbetet med samhällets informationssäkerhet.

MSB – Informationssäkerhet

Direktlänk till sidorna på MSB om informationssäkerhet. Här finns en hel del publikationer i form av vägledningar, handböcker m.m.

Informationssäkerhet.se

På informationssäkerhet.se finns stöd för hur man arbetar med systematisk informationssäkerhet i organisationer. Informationssäkerhet drivs av MSB i samverkan med PTS, Polisen, Säpo, FRA, FMV och Försvarsmakten.

CERT-SE

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

CERT-SE agerar operativt då IT-incidenter inträffar genom informationsspridning och samordning, samverkar med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet och är Sveriges kontaktpunkt gentemot andra länder.

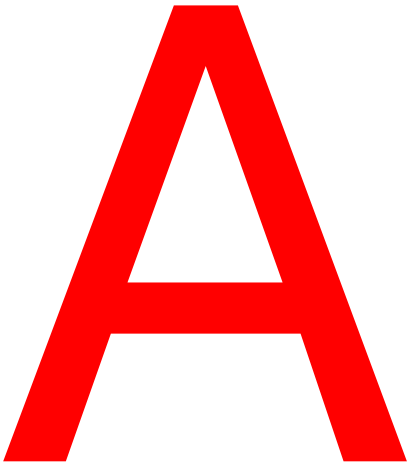
Dataföreningen

Dataföreningen har nätverk och utbildningar inom informationssäkerhet och ordnar seminarier m.m.

SIS - informationssäkerhet

SIS – Swedish Standards Institute – är Sveriges standardiseringsorgan och publicerar de svenska standarderna inom informationssäkerhetsområdet, främst den s.k. 27000-serien.

SIS ordnar seminarier och konferenser och ger utbildningar i Informationssäkerhetsakademin.



Kapitel A: Informationssäkerhet för medarbetare

Antagen av kommunstyrelsen 2024-06-11 § 91

Innehåll Kapitel A

Inledning

Detta kapitel vänder sig till alla medarbetare vid Sorsele kommun. Riktlinjerna gäller även förtroendevalda och extern personal som har åtkomst till Sorsele kommuns information, exempelvis inhyrda konsulter.

Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Sorsele kommun och vilka regler som gäller.

Sorsele kommun är en organisation med flera verksamheter. Verksamhetsspecifika kompletterande regler till riktlinjerna kan därför finnas. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

Informationssäkerhet för medarbetare följer i stort en struktur framtagen av Myndigheten för samhällsskydd och beredskap (MSB) som finns i en utbildning för informationssäkerhet: DISA (Datorstödd Informationssäkerhetsutbildning för användare).

Syftet är att man kan genomgå DISA-utbildningen och parallellt se vilka riktlinjer som gäller i Sorsele kommun.

DISA består av 10 avsnitt om informationssäkerhet, och alla avsnitt utgörs av en film med tillhörande information och frågor. Dessa riktlinjer består dock endast av åtta avsnitt (A1 – A8), eftersom information och regler gällande mobila enheter, smarta telefoner och surfplattor slagits samman till ett avsnitt (avsnitt A2).

Innan de åtta områdena utifrån DISA inleds kapitlet med följande avsnitt: Medarbetares ansvar för informationssäkerhet och Informationsklasser som även innehåller information om personuppgifter samt allmänna handlingar och sekretess.

DISA-utbildningen och dessa riktlinjer finns på sidan Informationssäkerhet på Sorsele kommuns intranät Hänna.

På denna sida finns information om arbetet med informationssäkerhet i Sorsele kommun samlad.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Sorsele kommun som är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör t.ex. förskolor, grundskolor, socialtjänst, hemvård, bygglov m.m. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av text, men även bilder, symboler, filmer och ljud utgör information.

Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada. Det finns en hel del lagar och föreskrifter som kommunen måste leva upp till, och privatpersoner, företag och andra har förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav.

Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, eller administrativt i form av regler (som dessa riktlinjer) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp m.m. Medarbetares kunskap och medvetenhet är ett avgörande 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. Säkerheten 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 Sorsele kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Sorsele kommun ställer krav på att medarbetare följer dessa riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare.

Om du som medarbetare eller externt kontrakterad har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att anställningen eller avtalet upphört.

Vid underlåtenhet att följa dessa riktlinjer för informationssäkerhet följer Sorsele kommun reglerna enligt lagar och avtal. Lagbrott polisanmäls.

Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på Sorsele kommuns information. Exempelvis:

- IT-angrepp/intrång
- Oskyddad känslig information
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet

IT- och informationsrelaterade incidenter och brister ska rapporteras till IT-enheten samt till din närmaste chef.

Antagen av kommunstyrelsen 2024-06-11 § 91

Informationsklasser

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga.

I Sorsele kommun finns tre klasser för hur känslig informationen är och hur den får spridas:
Allvarlig, Betydande, Måttlig. (Öppen, Intern eller Konfidentiell)[1]. Dessa illustreras i Figur 2.

		Konfidentialitet	**Riktighet**	**Tillgänglighet**
3	**Allvarlig konsekvens**	**K3** Information där förlust av konfidentialitet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R3** Information där förlust av riktighet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T3** Information där förlust av tillgänglighet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
2	**Betydande konsekvens**	**K2** Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R2** Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T2** Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
1	**Måttlig konsekvens**	**K1** Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R1** Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T1** Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

[1] Sorsele kommuns modell för informationsklassning som beskrivs i Kapitel B – Styrning av informationssäkerhet innehåller förutom konfidentalitet även aspekterna riktighet och tillgänglighet. För de flesta medarbetare är dock endast graden av konfidentialitet relevant så som det beskrivs i detta kapitel.

Olika regler gäller för dessa tre klasser vad gäller spridning och hantering av information:

- **Måttlig konsekvens/öppen information** har inga krav på åtkomstbegränsning utan kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, t.ex. på extern webbplats som www.sorsele.se.
- För **Betydande konsekvens/Intern information** gäller de normala hanteringsregler som finns nedan i avsnitt A1 – A8. Intern information kan normalt spridas internt inom kommunen. Om intern information sprids till extern aktör ska det finnas ett tydligt syfte med detta.
- Särskilda hanteringsregler gäller för **Allvarlig konsekvens/konfidentiell information.** I detta kapitel är all information och alla riktlinjer som gäller för **konfidentiell** information markerad med fetstil och med dubbla ramar i tabeller med riktlinjer.

Inom Sorsele kommun är idag långt ifrån all information klassad enligt de tre klasserna. Att klassa information på det här sättet är ett arbete som nyligen påbörjats. Det viktigaste är att **konfidentiell** information hanteras på rätt sätt. **Konfidentiell** information är bl.a. känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef.

Personuppgifter

Vid de flesta av Sorsele kommuns verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande förordningar så som Dataskyddsförordningen (GDPR) och Lagen om behandling av personuppgifter inom socialtjänsten.

Personuppgifter kan vara klassade som **konfidentiell**, intern eller öppen information. Det beror på sammanhang, vilka personuppgifter som avses osv. Dataskyddsförordningen skiljer mellan vanliga personuppgifter och känsliga personuppgifter. Normalt är det förbjudet att hantera känsliga personuppgifter, men det finns undantag från förbudet. Känsliga uppgifter måste också skyddas mer än andra uppgifter.

Känsliga uppgifter är uppgifter om

- etniskt ursprung
- politiska åsikter (till exempel uppgift om att du är med i ett visst politiskt parti)
- religiös eller filosofisk övertygelse (till exempel uppgift om att du tillhör en viss religion eller inte tillhör någon religion alls)
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person.

Känsligheten hos personuppgifter beror dock på flera faktorer och även mängden av uppgifter om varje person måste beaktas eftersom den bestämmer hur detaljerad bild av en person som kan erhållas. Det innebär att flera personuppgifter som var för sig inte bedöms känsliga tillsammans kan bilda känsliga personuppgifter.

Skyddade personuppgifter är alltid **konfidentiell** information och ska hanteras utifrån särskilda rutiner och regler.

Allmänna handlingar och sekretess

En handling är allmän om den är förvarad, inkommen till, eller upprättad hos kommunen och ska diarieföras. Allmänheten ska kunna ta del av allmänna handlingar och kommunen är skyldig, efter sekretessprövning, att ha tillgång till dessa för att skyndsamt tillhandahålla den i läsbar form till den som så begär det.

Allmänna handlingar kan vara både i form av analog och digital information och ska hanteras, bevaras och gallras i enlighet med kommunens dokumenthanteringsplan.

Information som är allmän handling kan vara sekretessbelagd enligt offentlighets- och sekretesslagen. Sådana handlingar får inte lämnas ut utan att en sekretessbedömning har gjorts.

Arbetsmaterial under ett ärendes beredning, minnesanteckningar, verksamhetsinterna meddelanden och personliga meddelanden är normalt inte allmänna handlingar. Denna information kan klassas som **konfidentiell**, intern eller öppen information beroende på känslighet, t.ex. utifrån krav från författningar.

A1. Lösenord

För att logga in till de flesta av Sorsele kommuns IT-system används användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn.

Via Sorsele kommuns nätverk blir du påmind om när lösenord behöver bytas och via IT-enheten kan du få ett nytt om du har glömt ditt lösenord.

Användar-ID och lösenord används för att skydda information som kan vara intern eller **konfidentiell**, och det är därför viktigt att följa nedanstående regler för skapande och hantering av lösenord.

Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet. Krav på lösenord:

Riktlinjer för utformning av lösenord för medarbetarkonto	
A.1.1	Lösenord ska vara minst 12 tecken långt, gärna längre.
A.1.2	Lösenord ska innehålla en blandning av stora och små bokstäver, siffror och symboler.

Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:

Mening:	Lösenord:
Klockan 10 går två bilar till Sorsele ! jag åker med	K10g2btS!jåm

Användar-ID och lösenord är i sig viktig information där Användar-ID är intern information medan lösenord är **konfidentiell** information och ska hanteras på ett säkert sätt.

Riktlinjer för hantering av lösenord	
A.1.3	Lösenord ska inte vara synliga. Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp.
A.1.4	Lösenord för andra tjänster ska rekommenderat också vara 12 tecken långt. Olika lösenord ska användas. Olika lösenord ska användas för olika tjänster på webben även om de är jobbrelaterade.
A.1.5	Samma lösenord ska inte användas privat och i jobbet. På så vis minskas riskerna att någon kommer åt information.
A.1.6	Lösenord till Användar-ID ska bytas 1 gång per år, systemet framtvingar lösenordsändringen. Om man arbetar i system där lösenordsbyte inte är tvingande, ska man ändå byta ut lösenordet minst 1 gång per år. Lösenord ska bytas direkt om misstanke finns att det har avslöjats.

A.1.7	Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.
A.1.8	Automatisk minnesfunktion för lösenordet får användas med förutsättning att lösenorden inte återanvänds på flera sidor/tjänster. Det är särskilt viktigt att inte spara lösenord via lösenordshanterare då en dator delas av flera. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/ta bort lösenord, vilken kan användas om man är osäker på om lösenord har lagrats.

A2. Mobila enheter

Den IT-utrustning som tillhandahålls av Sorsele kommun kan vara stationär eller bärbar, en så kallad mobil enhet. Mobil enhet avser bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta.

Applikationsspecifika datorer, mobiler eller surfplattor kan ha specifika riktlinjer utöver dessa som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Riktlinjer för hantering av mobila enheter	
A.2.1	Mobila enheter som tillhandahålls av Sorsele kommun är personliga arbetsredskap och får inte lånas ut eller överlåtas om det inte är enheter av verksamheten ska delas av flera.
A.2.2	Uppsatta säkerhetsinställningar i enheter får inte ändras.
A.2.3	Endast godkända programvaror får installeras på enheten.
A.2.4	Installerad programvara får inte kopieras eller installeras på annan enhet.
A.2.5	Mobila enheter ska låsas med lösenord/skärmlås.
A.2.6	**Konfidentiell** information måste vara krypterad på mobila enheter.
A.2.7	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras.
A.2.8	Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
A.2.9	Gästers utrustning och annan övrig utrustning kan anslutas till kommunens gästnät Public.
A.2.10	Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade. Inga enheter får anslutas till publika öppna wifi nätverk.
A.2.11	Vid distansarbete måste godkänd säker utrustning och anslutning användas.
A.2.12	Vid distansarbete utanför Sverige, i Europa, måste dialog med IT-enheten ske i god tid innan avresa.
A.2.13	Vid planerat distansarbete utanför Europa, görs säkerhetsbedömning om möjlighet finns från fall till fall av IT-enheten. Det är därför av stor vikt att ha en dialog i god tid innan avresa.
A.2.14	Anslutning med kommunens VPN-anslutning från en privat dator är ej tillåtet.
A.2.15	Anslutning via VPN ska ske genom den säkraste lösningen som erbjuds.
Riktlinjer för fysisk hantering av mobila enheter	

A.2.12	Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
A.2.13	Arbete med **konfidentiell** information får inte ske i publika miljöer.
A.2.14	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
A.2.15	Förlust av enhet ska omedelbart anmälas till IT-enheten, polisanmälan sker via verksamhetsansvarig. I vissa fall finns möjligheter att fjärradera information.
A.2.16	Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat.
A.2.17	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt.

Särskilda regler för smarta telefoner och surfplattor

Förutom de regler som gäller allmänt för mobila enheter gäller även följande vid användning av smarta telefoner och surfplattor:

Regler för smarta telefoner och surfplattor	
A.2.18	Sorsele kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som används i tjänsten och även till den information som finns i dessa. Man bör därför som medarbetare vara medveten om att arbetsgivaren har rätt att ta del av t.ex. sms, foton och kalenderanteckningar. Eftersom offentlighetsprincipen gäller kan det vara möjligt för utomstående att begära ut informationen.
A.2.19	Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. I syfte att minska denna risk är det endast tillåtet att ladda ned appar från Sorsele kommuns interna appkatalog, App Store eller Google Play.
A.2.20	Information som är **konfidentiell** får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används.
A.2.21	Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till bankomatkort.
A.2.22	Vårda utrustningen och använd exempelvis skärmskydd och skal.

A3. Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke, och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

Skadlig kod är ett växande problem och den blir mer och mer sofistikerad och ”intelligent” och kan vara svår att upptäcka och kan utföra avancerade operationer. Man behöver idag inte vara en teknisk kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på Internet.

Exempel på idag förekommande skadlig kod:

- Trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare.
- Maskar, självproducerande program, sprids genom nätverk och kan överbelasta.
- Ransomware, där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma.

Spridning av skadlig kod

I dagens digitala vardag är risken för skadlig kod som sprids till datorer och mobila enheter verklig. Att öppna e-postbilagor, importera filer eller surfa på internet och klicka på länkar, inklusive de som delas i sociala medier, kan vara en potentiell källa till infektion.

Avsändare av e-post kan fortfarande fejkas och webbsidor är inte alltid vad de verkar vara. Identitetsstölder, särskilt på plattformar som Facebook, är fortfarande en risk, och e-postadresser kan fortfarande förfalskas i syfte att lura mottagare till att klicka på länkar. Phishing-attacker, där mottagaren luras att ange koder, lösenord eller bankinformation på falska sidor, är vanliga. Det är viktigt att vara medveten om detta och undvika att lämna ut sådana känsliga uppgifter. Seriösa organisationer, inklusive myndigheter och företag, begär aldrig känslig information på detta sätt.

Infektion av IT-utrustning, kan utgöra en betydande risk. Om en infekterad enhet ansluts till kommunens nätverk kan skadlig kod sprida sig och orsaka omfattande skador. Även om kommunens datorer är utrustade med skydd mot skadlig kod, är det viktigt att förstå att detta inte ger fullständig säkerhet, eftersom dessa typer av hot utvecklas snabbt.

För att minimera riskerna bör användare vara vaksamma och hålla sig informerade. Uppdaterade säkerhetsåtgärder är avgörande för att skydda sig mot dagens mer avancerade digitala hot.

Riktlinjer för skydd mot skadlig kod	
A.3.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
A.3.2	Anslut endast godkänd IT-utrustning till kommunens nätverk.
A.3.3	Var misstänksam och undvik att klicka på konstiga länkar eller fylla i irrelevanta uppgifter.
A.3.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad.
A.3.5	Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta IT-enheten.

A4. Internet och sociala medier

Användning av Internet och sociala medier kan vara till stor nytta och glädje, privat såväl som på arbetet. Förutom de riktlinjer som är kopplade till skadlig kod i avsnitt A3 finns här särskilda regler för användning av Internet och sociala medier.

Riktlinjer för Internetanvändning	
A.4.1	Internet är i arbetet på Sorsele kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
A.4.2	De regler som gäller i samhället i övrigt gäller självklart även inom Sorsele kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som ibland måste beaktas när man använder Internet.
A.4.3	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, bilder, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
A.4.4	I begränsad omfattning får Internet användas för privata syften. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Sorsele kommuns nätverk.
A.4.5	Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller **konfidentiell** information.

Sorsele kommuns etiska regler och värderingar ska följas även vid kommunikation via Internet och sociala medier, när man som kommunanställd kommunicerar som officiell representant för kommunen. Tänk därför på att:

Etiska riktlinjer	
A.4.6	All kommunikation på Internet från Sorsele kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte.
A.4.7	Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.

Inlägg på Sorsele kommuns sociala medier har potential att nå ett stort antal följare. Kommunens sociala medier utgör också ett av kommunens viktiga kommunikationssystem och intrång kan få stora konsekvenser för kommunorganisationens förtroende och pålitlighet.

Riktlinjer för sociala medier	
A.4.8	Anställda med åtkomst till kommunens sociala medier ska tillämpa multifaktorautentisering för inloggning, även i de fall privata profiler används för inloggning.

A5. E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med e-post normalt är helt öppen. Att sända e-post som inte är skyddad, t.ex. med kryptering, kan jämföras med att skicka vykort.

Ansvar

A.5.1	Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
A.5.2	Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas, annan ska bevaka e-postlådan, och om nödvändigt hänvisning till kollega eller chef. Vid avslut av anställning eller vid tjänstledighet tas e-posten bort.
A.5.3	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (kommun@sorsele.se) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.

Allmänna handlingar	
A.5.4	E-post som skickas till personliga brevlådor är allmän handling om innehållet är arbetsrelaterat. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas. Huvudregeln är att e-post som är allmän handling omgående ska vidarebefordras till registrator/kansliet.
A.5.5	E-post som är allmän handling får gallras, dvs. raderas, först när e-posten diarieförts. Vissa epostmeddelanden som är allmänna handlingar är av uppenbar ringa eller tillfällig betydelse och är undantagna från kravet på registrering.

Privat e-post	
A.5.6	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd inte ditt epostkonto i Sorsele kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsmaterial.
A.5.7	Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser.

E-post och konfidentiell information	
A.5.8	Öppen och intern information får skickas med e-post, medan **konfidentiell** information endast får skickas med e-post som använder av Sorsele kommun godkänd kryptering.
A.5.9	Dokument som skannas skickas ofta med e-post från skannern till mottagarens e-postadress. Skanning av dokument som innehåller **konfidentiell** information ska även den krypteras av Sorsele kommun godkänd kryptering.

A6. Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering m.m.

Riktlinjer för lagring och säkerhetskopiering	
A.6.1	Information ska lagras enligt aktuell informationshanteringsplan/dokumenthanteringsplan. Information ska annars lagras på nätverket så att den säkerhetskopieras. Det kan vara personliga (Z:) eller gemensamma filytor/mappar (för närvarande Grupper eller Z:, H:, K: osv.).

A.6.2	Om information behöver lagras på lokal hårddisk (C:), se till att regelbundet kopiera över informationen till nätverket.
A.6.3	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska IT-enheten skyndsamt kontaktas för undersökning om möjlighet finns att återskapa den senaste säkerhetskopian.
A.6.4	**Konfidentiell** information får endast lagras i därför avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
A.6.5	Lokal lagring av **konfidentiell** information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Sorsele kommun godkänd metod för kryptering.
A.6.6	Fysiska dokument som innehåller **konfidentiell** information ska förvaras inlåsta.

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror.

Riktlinjer för lagring i molntjänster	
A.6.6	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
A.6.7	**Konfidentiell** information får inte lagras i personliga molntjänster.

A7. Spårbarhet och loggning

Loggning sker i kommunens datorer och nätverk. Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer.

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn.

All Internettrafik och e-post loggas centralt. Sorsele kommun har som arbetsgivare rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

A8. Säkert beteende

En stor del av kommunens information hanteras muntligt och på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar **konfidentiell** information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara t.ex. omdömen om chefer och medarbetare eller information om en oförutsedd händelse, t.ex. ett brott. Sådan information kan vara känslig och är i så fall **konfidentiell** information.

Riktlinjer för muntlig information	
A.8.1	**Konfidentiell** information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer och i informella sammanhang, till exempel vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
A.8.2	Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på öppen plats, eller i telefonsamtal i kassakön. **Konfidentiell** information får överhuvudtaget inte kommuniceras muntligt i publika lokaler.

Riktlinjer för information på skärmar och i pappersform	
A.8.3	Skriftligt material som innehåller **konfidentiell** information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder.
A.8.4	**Konfidentiell** information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund.
A.8.5	Besökare får inte vistas utan uppsikt i lokaler där **konfidentiell** information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler.
A.8.6	Vid fysisk posttjänst ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller **konfidentiell** information.
A.8.7	Då **konfidentiell** information överförs via fax ska man försäkra sig om att man har rätt nummer (t.ex. använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
A.8.8	Vid utskrift ska dokument omgående hämtas upp ur skrivare. För MFP skrivare ska utskriften taggas ut. Vid utskrift av **konfidentiell** information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen.
A.8.9	Pappersdokument som innehåller **konfidentiell** information måste vid kassering strimlas eller förstöras genom godkända metoder.