Diarienummer
KS 2023-00349

Antagna av kommunstyrelsen KS § 349/231121.

# Riktlinjer för informationssäkerhet i Söderhamns kommun

| | |
|---|---|
| Beslutat av<br>Kommunstyrelsen | Gäller för |
| Revideringshistorik | Rättslig eller annan grund |
| Ersätter | Dokumentägare |
| Nästa revidering<br>2026-02-01 | Dokumentansvarig |

# Innehåll

# Riktlinjer för informationssäkerhet i Söderhamns kommun

## Inledning

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

Dessa riktlinjer är fastställda av kommunstyrelsen och gäller från och med 2023-12-01

## Riktlinjernas omfattning

Dessa riktlinjer gäller för informationssäkerhet inom Söderhamns kommun inklusive de bolag, stiftelser och ekonomiska föreningar där kommunen utövar ett rättsligt bestämmande inflytande. Riktlinjerna ska även tillämpas av dem som har beroenden till kommunens gemensamma informationstillgångar.

Riktlinjerna innehåller information och regler gällande säkerhet vid all hantering av information inom Söderhamns kommun. Riktlinjerna gäller för alla verksamheter i Söderhamns kommun, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa.

## Struktur och läsanvisningar

För att ge god läsbarhet är dokumentet uppdelat i fyra kapitel (A-D) som riktar sig till olika målgrupper:

### A Informationssäkerhet för medarbetare

Information och riktlinjer för hur information och IT ska hanteras i olika situationer. *Gäller alla medarbetare.*

### B Styrning av informationssäkerhet

Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas. *Gäller alla verksamhetsansvariga, informationsägare samt alla som arbetar med IT- eller informationssäkerhet.*

### C Informationssäkerhet i verksamhetsnära förvaltning

Information och riktlinjer för informationssäkerhet i förvaltningsobjekt som t ex. system och grupper av system. *Gäller i första hand informationsägare, objektägare och sektorledare.*

### D Informationssäkerhet i IT-miljön

Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT- och informationssäkerhet. *Gäller chefer och medarbetare inom IT-sektorn.*

Varje kapitel består både av informativa avsnitt och av riktlinjer som är obligatoriska.

Samtliga riktlinjer är numrerade och i tabellform. Rader som innehåller riktlinjer för konfidentiell information och höga skyddskrav har röda linjer, tjockare linje och nämnda termer är dessutom fetmarkerade.

Exempel från Kapitel A om lagring i molntjänster:

**Riktlinjer för lagring i molntjänster.**

| | |
|---|---|
| A 5.12 | Söderhamns kommuns information får inte lagras i personliga molntjänster typ Dropbox m fl. |
| A 5.13 | Hög sekretess (Röd) information får inte lagras i molntjänster |

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.

Söderhamns 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. Liksom vår informationssäkerhetspolicy är dessa

riktlinjer baserade på den svenska och internationella standarden SS-ISO/IEC 27002.

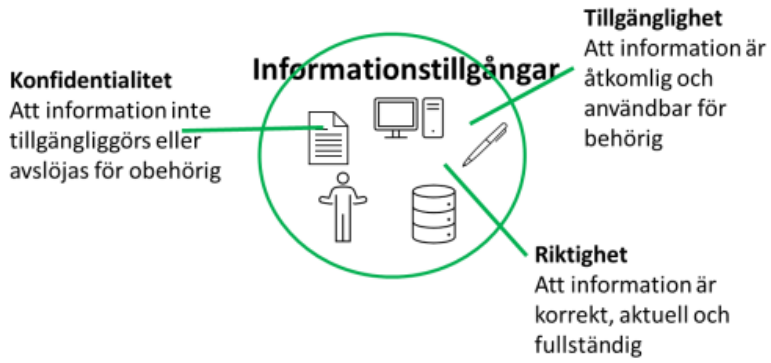
## Introduktion till informationssäkerhet

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 tre aspekter; att informationstillgångar ska vara konfidentiella, riktiga och tillgängliga. (Figur 1)

*Figur 1*




Olika typer av händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialiteten, riktigheten eller tillgängligheten hos informationstillgångar. Information kan på ett oönskat sätt till exempel stjälas, raderas, förändras, avslöjas för obehöriga eller göras otillgänglig.

En viss informationstillgång 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 som ofta inbegriper 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 informationstillgång beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

## Termer och definitioner

Termer inom Informations- och IT-säkerhet är beskrivna i tabell på kommande sidor.

| 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 | Omtolkningsbar framställning av information på ett formaliserat sätt lämpligt för kommunikation, tolkning eller bearbetning. |
| E-postbluff/E-mail spooling | En form av spam eller phishing, där kriminella avsändare förfalskar avsändarens e-postadress till en e-postadress som mottagaren litar på i syfte att orsaka skada i någon form |
| IKT | Informations- och Kommunikationsteknik |
| Incident | Enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten |
| Information | Kunskap om objekt, såsom fakta, händelser, saker, processer eller idéer, inklusive begrepp, som inom ett visst sammanhang har en särskild betydelse. |
| Informationsklassning | Att genom konsekvensanalys identifiera skyddsbehovet för en viss information |
| Informationssäkerhet | Bevarande av informationens konfidentialitet, riktighet och tillgänglighet |
| Informationssäkerhetsincident | Enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet |
| Informationssäkerhetspolicy | Organisationens viljeinriktning med informationssäkerhet uttryckt av organisationens ledning. |
| Informationstillgång | En mängd information, definierad och hanterad som en enda enhet, så att den kan förstås, delas, skyddas och utnyttjas effektivt. Informationstillgångar har Informationsklass: Öppen 9 (100) igenkännligt och hanterbart värde, risk, innehåll och livscykler. |
| 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 | Ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. |
| Mobila enheter | Lättportabla IT-resurser såsom bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta. |
| Molntjänst | Molnbaserad tjänst, (på engelska: cloud-based service) – tjänst som tillhandahålls via Internet från ett nätverk av servrar. I princip ska användaren inte behöva ha mer än en webbläsare och internetanslutning för att använda tjänsten. |
| Outsourcing | Utläggning av delar av ett företags eller myndighets produktion eller annan verksamhet till ett annat företag. |
| Riktighet | Att information är korrekt, aktuell och fullständig. |
| Sekretess | Förbud att i offentlig verksamhet röja uppgifter muntligen eller genom utlämnande av allmän handling. Regler om sekretess finns i offentlighets- och sekretesslagen respektive offentlighets- och sekretessförordningen. |
| Skadlig kod/program/Maleware | En form av programvara som kriminella har skapat i syfte att infektera datorer och andra enheter. Detta kan t.ex. vara virus, trojaner, maskar, ransomware, spyware och adware |
| Spårbarhet | Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs. |
| Stark autentisering | Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet. |
| Tillgänglighet | Att information är åtkomlig och användbar av behörig. |
| Verksamhetskritiska system | Kritiska system som har klassats med höga krav på konfidentialitet, integritet och/eller tillgänglighet. |

# Kapitel A Informationssäkerhet för medarbetarna

**Innehåll Kapitel A**



## Inledning

Detta kapitel vänder sig till alla medarbetare i Söderhamns kommun. Riktlinjerna gäller även extern personal som har åtkomst till Söderhamns kommuns information, exempelvis inhyrda konsulter. Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Söderhamns kommun och vilka regler som gäller.

Söderhamns kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller. Dessa riktlinjer finns på kommunens intranät, sidan för informationssäkerhet. På den sidan finns all information samlad om vårt arbete med informationssäkerhet i kommunen.

## A1. Övergripande regler

Följande regler är övergripande och sammanställer grundläggande informationssäkerhetskrav på medarbetare:

**Övergripande regler**

| | |
|---|---|
| A 1.1 | Medarbetare ska vara medveten om sin skyldighet att rapportera informationssäkerhetsincidenter och -brister i Söderhamns kommuns informationshantering och IT-säkerhet. Detta ska göras till Servicedesk eller till närmaste chef. En incident som rör personuppgifter rapporteras till närmaste chef eller direkt till informationssäkerhetsansvarig. Genom incidentrapporteringen har vi chans att förbättra vårt informationssäkerhetsarbete. En incident kan vara skadlig kod (virus), att personuppgifter har hamnat i orätta händer eller hanterats felaktigt, ett dataintrång eller stöld och förlust av utrustning innehållandes information |
| A 1.2 | Som medarbetare har du ansvar att kontrollera handlingens informationsklass så att du kan vara säker på att informationen får rätt skydd. Informationsklass kan vara noterat på sidhuvud/sidfot eller elektroniskt i systemet. |

| | |
|---|---|
| A 1.3 | Lösenordet som medarbetare skapar för sin inloggning i Söderhamns kommuns nätverk ska ha minst 9 tecken. |
| A 1.4 | Det är otillåtet att dela på personliga konton. Varje individ måste kopplas till och vara ansvarig för sina handlingar. Delar du ditt konto så blir du ansvarig för den aktivitet som kan kopplas till kontot, oavsett om det var någon annan som utförde handlingen eller inte. |
| A 1.5 | Medarbetare ska bara öppna länkar eller bifogade filer i e-postmeddelanden från betrodda avsändare. Det absolut vanligaste sättet att sprida skadlig kod för att stjäla information eller sabotera är att lura användare att klicka på länkar eller öppna bifogade filer i e-post. |
| A 1.6 | Medarbetare får inte använda e-postadresser med domännamnet soderhamn.se för privat bruk som registrering av ett privat konto i kommersiella tjänster. Sådan registrering kan medföra att Söderhamns kommun får krav på att teckna företagslicens för nyttjande av tjänsten. |
| A 1.7 | Genom att låsa din dator (CTRL + ALT + DEL, Välj Lås) eller (Windowstangent + L) medverkar du till att skydda känsliga uppgifter mot obehörig insyn och förändring. Exempelvis när personer passerar eller går in till ditt arbetsrum. Detta ska du göra varje gång du lämnar din dator obevakad, även för korta stunder. |
| A 1.8 | Söderhamns kommuns medarbetare ska följa svensk lag och kommunens interna riktlinjer vid internetanvändning. |
| A 1.9 | Som medarbetare har du rätt till skydd för din kommunikation och ditt privatliv. Men vid allvarlig misstanke om illojalt eller brottsligt beteende kan det vara tillåtet för arbetsgivaren att ta del av själva innehållet inte bara i arbetsrelaterat material utan även i dina privata filer eller e-postmeddelanden som finns i kommunens IT-miljö. Chef har till ansvar att se till att du som medarbetare är medveten om detta. |
| A 1.10 | Medarbetaren ska ha kännedom om och tagit del av de styrdokument som berör medarbetarens arbete. Dessa finns publicerade på Söderhamns kommuns intranät och/eller kvalitetsledningssystem eller dylikt. Chef ansvarar för att ge medarbetare en introduktion till de styrande dokument som gäller. |
| A 1.11 | Under distansarbete behöver du som medarbetare ta stort eget ansvar för att skydda kommunens information mot obehörig åtkomst. |

**Medarbetares ansvar för informationssäkerhet**

Information är en viktig resurs för Söderhamns 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 till exempel förskolor, grundskolor, socialtjänst, hemsjukvård, stadsplanering, biblioteksservice, bygglov med mera. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av texter, 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 men också om sådan information som skulle kunna skada organisationen eller samhället om den sprids.

Det finns en hel del lagar och föreskrifter som kommunen måste leva upp till. 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 med mera.

Även medarbetares kunskap och medvetenhet är ett nog så viktigt skydd, till exempel att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information som till exempel känsliga 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 Söderhamns kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

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

Som anställd i Söderhamns kommun omfattas du av en straffsanktionerad tystnadsplikt. Denna tystnadsplikt gäller även efter att din anställning upphört. Grundlagsstadgat finns din rätt att offentliggöra uppgifter enligt meddelarfriheten, med de begränsningar som finns i offentlighets- och sekretesslagen.

Om du är externt kontrakterad och har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att avtalet upphört. Vid underlåtenhet att följa dessa riktlinjer för informationssäkerhet följer Söderhamns kommun gällande regler enligt lagar och avtal. Lagbrott polisanmäls.

**Skyldighet att rapportera incidenter och brister.**
Alla medarbetare har skyldighet att rapportera informationssäkerhetsincidenter eller brister som misstänkts kunna medföra negativ påverkan på Söderhamns kommuns information. Det kan röra sig om t.ex.

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

IT- säkerhetsrelaterade incidenter och brister ska rapporteras till Servicedesk (766 99). Rör incidenten personuppgifter så ska detta rapporteras enligt A 1.1 Meddela även din chef. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga, ska dock inte själva försöka bevisa sådana då det kan försvåra framtida utredningar. Det är bra att dokumentera iakttagelser i samband med upptäckten av incidenten.

Informationssäkerhetsansvarig sammanställer en incidentrapport en gång per år som rapporteras till kommundirektörens ledningsgrupp och berörda verksamheter.
Rapporten omfattar:

- Intrång och försök till intrång
- Brott mot lagstiftning och internt regelverk
- Incidenter som orsakar eller skulle kunna orsaka betydande avbrott eller störningar
- Konsekvenser och förslag till åtgärder efter intrång eller funktionsfel

**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 Söderhamns kommun finns fyra klasser för hur känslig informationen är och hur den får spridas: Öppen, Begränsad, Känslig-Sekretess eller Hög Sekretess. Dessa illustreras i Figur 2.

| Informationsklass | Behörighet/spridning | Exempel |
|---|---|---|
| 4 Hög Sekretess (Röd) | Endast ett mycket begränsat antal behöriga personer | Skyddade personuppgifter, information som om den hamnar i orätta händer medföra fara för liv och hälsa eller samhällsskada |
| 3 Känslig-Sekretess (Gul) | Endast den som behöver informationen för att klara sin arbetsuppgift, särskild åtkomstbegränsning med god spårbarhet | Känsliga personuppgifter, integritetskänsliga (extra skyddsvärda) såsom personnummer och sociala förhållanden, information under pågående upphandling, skalskyddsritningar |
| 2 Begränsad (Grön) | Normal åtkomstbegräsning med viss spårbarhet | Allmänna personuppgifter, allmänna offentliga handlingar, födelsedata (6 första siffrorna i personnummer YYMMDD) |
| 1 Öppen (Vit) | Ingen åtkomstbegränsning | Handlingar utan direkta eller indirekta personuppgifter |

*Figur 2 I Söderhamns kommun används fyra informationsklasser*

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

- Öppen (Vit) information kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, t.ex. på extern webbplats som www.soderhamn.se.
- För Begränsad (Grön) information gäller normal åtkomstbegräsning och de normala hanteringsregler som finns nedan i avsnitt A1 – A9. Grön information kan normalt spridas internt inom kommunen och externt. Grön är en markering att informationen kan innehålla personuppgifter.
- För Känslig-Sekretess (Gul) information gäller särskilda åtkomsträttigheter och hanteringsregler. I detta kapitel är all information och alla riktlinjer som gäller för känslig information markerad med fetstil och med röda ramar i tabeller med riktlinjer. Om känslig information delas till extern aktör ska det finnas ett tydligt syfte med detta. Känslig information får bara delas till betrodda externa parter.
- För Hög Sekretess (Röd) information gäller mycket begränsade åtkomsträttigheter och minimal spridning. Uppgifterna kräver ofta strikt manuell hantering och ska så långt det är möjligt hållas borta från digitala miljöer. Uppgifter i denna klass kan om de sprids medföra fara för liv och hälsa för den som uppgifterna avser eller för en stor mängd individer. Även dessa är markerade med fetstil, tjockare ram och röd ram.

Det finns dessutom information som är klassat högre än Hög sekretess (Röd), sådan information regleras av säkerhetsskyddslagstiftning. Observera att särskilda regler finns för hantering av sådan information, kontakta Söderhamns kommuns säkerhetsskyddschef.

Inom Söderhamns kommun är idag långt ifrån all information klassad enligt de fyra klasserna. Att klassa information på det här sättet är ett arbete som startades under 2019 i DraftIT. Fortsättningsvis arbetar vi i Klassa 4.0 Det viktigaste är att Känslig-Sekretess (Gul) och Hög Sekretess (Röd) information hanteras på rätt sätt. Det är bl.a. känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef eller kommunens digitaliseringsstrateg.

**Personuppgifter**
Vid de flesta av Söderhamns kommuns verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande författningar bl. a EU ´s dataskyddsförordning (GDPR) och Lagen om behandling av personuppgifter inom socialtjänsten. Personuppgifter kan vara klassade som Hög Sekretess (Röd), Känslig-Sekretess (Gul) eller Begränsad (Grön) information. Det beror på sammanhang, vilka personuppgifter som avses osv. Känsliga personuppgifter är dock alltid lägst klassade som Känslig-Sekretess (Gul) information.

- Till känsliga personuppgifter räknas uppgifter som avslöjar:
- Ras eller etniskt ursprung
- politiska åsikter,
- religiös eller filosofisk övertygelse,

- medlemskap i fackförening,
- genetiska uppgifter,
- biometriska uppgifter för att entydigt identifiera en fysisk person,
- uppgifter om hälsa,
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Utöver känsliga personuppgifter finns det också personuppgifter som Integritetsskyddsmyndigheten (IMY) kallar särskilt skyddsvärda. Detta är inte känsliga personuppgifter men uppgifter som IMY bedömt ändå kan orsaka stor skada ifall de inte hanteras korrekt.

För särskilt skyddsvärda personuppgifter gäller en högre teknisk säkerhet än för ”vanliga” personuppgifter. T.ex. får särskilt skyddsvärda personuppgifter inte skickas via okrypterad e-post utan det måste säkerställas att endast avsedd mottagare kan ta del av personuppgifterna. Särskilt skyddsvärda personuppgifter klassas som Känslig-Sekretess (Gul) information. Exempel på särskilt skyddsvärda personuppgifter är;

- personnummer,
- vissa löneuppgifter,
- uppgifter om lagöverträdelser,
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler,
- information som rör någons privata sfär,
- uppgifter om sociala förhållanden

Skyddade personuppgifter är alltid Hög Sekretess (Röd) information och ska hanteras utifrån särskilda rutiner och regler. Fråga din chef om den verksamhet du arbetar i har särskilda rutiner för skyddade personuppgifter.

**Allmänna handlingar och sekretess**
En handling är allmän och ska registreras om den är förvarad, inkommen till, eller upprättad hos kommunen. Om handlingen omfattas av sekretess måste den diarieföras. Allmänheten ska kunna ta del av allmänna handlingar och kommunen är skyldig att, efter sekretessprövning, 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 verksamheternas informationshanteringshanteringsplaner. Information som är allmän handling och sekretessbelagd enligt offentlighets- och sekretesslagen ska klassas som **Känslig-Sekretess** (Gul) eller **Hög Sekretess** (Röd) information.

Arbetsmaterial under ett ärendes beredning, minnesanteckningar, verksamhetsinterna meddelanden och personliga meddelanden är normalt inte allmänna handlingar. Denna information kan klassas som Hög Sekretess (Röd), Känslig-Sekretess (Gul), Begränsad (Grön) eller Öppen (Vit) information beroende på känslighet, t.ex. utifrån krav från författningar.

## A2. Lösenord

**Riktlinjer för utformning av lösenord**

| | |
|---|---|
| A 2.1 | Lösenord som du skapar för din inloggning till Söderhamns kommuns nätverk ska vara minst 9 tecken långt. |
| A 2.2 | Söderhamn Nära testar regelbundet lösenordets kvalitet |

| | |
|---|---|
| A 2.3 | Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet. Behövs tekniskt stöd för att lättare hålla ordning på lösenord så kan man använda en så kallad lösenordshanterare. Det finns säkra och avgiftsfria lösenordshanterare på marknaden, kontakta servicedesk för tips om sådana verktyg. |
| A 2.4 | Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information. |
| A 2.5 | Lösenord ska bytas direkt om misstanke finns att det har röjts. |
| A 2.6 | Lösenord till ett personligt användarkonto 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 2.7 | Om en dator delas av flera är det viktigt att automatisk minnesfunktion för lösenordet inte används. Om man loggar in på webbsidor så ska man då inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. 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. |

För att logga in till de flesta av Söderhamns 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. Hamnar ett lösenord i orätta händer kan det orsaka stor skada.

De flesta webbläsare har automatiska minnesfunktioner för att minnas de lösenord som du matar in. Ta för vana att **inte** spara lösenord i dina webbläsare med automatik eftersom då kan andra som har tillgång till din dator logga in på dina sidor. De flesta webbläsare har en funktion där du kan ta bort sparade lösenord. Via Söderhamn Nära blir du påmind om när lösenord behöver bytas och kan återställa till 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. Tips: Ett sätt att skapa ett

lösenord med bra kvalitet (starkt lösenord) kan vara att använda följande knep: Skapa ett starkt lösenord genom att sätta ihop slumpmässiga ord som tillsammans blir minst 9 tecken långt.

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

## A3. E-post

**Ansvar**

| | |
|---|---|
| A 3.1 | Din personliga brevlåda fornamn.efternamn@soderhamn.se är din tjänstebrevlåda. |
| A 3.2 | Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den mejl som skickas från kontot. |
| A 3.3 | E-postkonton kan stängas vid misstanke om brott eller missbruk |
| A 3.4 | E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga. |
| A 3.5 | Mejl ska klassificeras enligt Söderhamns kommuns klassificeringsmodell |
| A 3.6 | Skriv inte känsliga uppgifter i ämnesraden, eftersom inkorgens register över inkomna e-postmeddelanden räknas som allmän handling. |
| A 3.7 | Ska du skicka mejl till större grupper så ska du använda dig av funktionen ”Hemlig kopia”. Om du använder ”hemlig kopia” när du skickar mejl till större grupper undviker du att någon råkar skicka sitt svar till alla i gruppen trots att det bara var ämnat för dig som avsändare. Dessutom avslöjar du inte andras mejladresser om du använder ”hemlig kopia”. |
| A 3.8 | Om du får hotelsebrev via mejl ska du spara mejlet och kontakta din chef. |
| A 3.9 | Vid avslut av anställning tas e-postkontot bort efter viss tid, se därför till att mejl som din verksamhet kan behöva efter du har slutat din anställning sparas och lämnas över till annan handläggare. |

**Privat e-post**

| | |
|---|---|
| A 3.10 | Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via epost. Använd inte ditt epostkonto i Söderhamns kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsrelaterat material. |
| A 3.11 | Det är inte tillåtet att automatiskt vidarebefordra din personliga kommunala e-postbrevlåda till externa e-postadresser. |

**E-post och känslig information**

| | |
|---|---|
| A 3.12 | **Känslig – Sekretess (Gul)** information får inte hanteras i O365 mejl. |
| A 3.13 | Information som klassificerats som **Hög sekretess (Röd)** får inte hanteras i O365 mejl. |
| A 3.14 | Dokument som skannas skickas ofta med mejl från skannern till mottagarens e-postadress. Skanning av dokument som innehåller **känslig - sekretess (gul)** och **Hög Sekretess (Röd** ska hanteras via |

| | |
|---|---|
| | säker digital kommunikation (SDK) mellan myndigheter eller med digital post till medborgare. |
| A 3.15 | Om mejl inkommer som innehåller **känslig - sekretess (gul)** och **Hög Sekretess (Röd)** ska denna genast flyttas till verksamhetssystem. Svara inte avsändaren eller vidarebefordra ej i samma mejlkonversation, utan påbörja ny mejltråd utan känslig och sekretessinformation. Varpå meddelandet ska raderas från e-postklienten |
| A 3.16 | Om mejl inkommer som innehåller **Hög Sekretess (Röd)** ska denna genast överföras till verksamhetssystem. Varpå meddelandet ska raderas från e-postklienten. |

E-post (mejl) 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 mejl normalt är helt öppen. Att sända mejl som inte är skyddad, t.ex. med kryptering, kan jämföras med att skicka vykort.

## A4. Chatt/direktmeddelanden

**Chat och känslig information**

| | |
|---|---|
| A 4.1 | **Känslig – Sekretess (Gul)** information får inte hanteras i chatt. |
| A 4.2 | Information som klassificerats som **Hög sekretess (Röd)** får inte hanteras i chatt. |
| A 4.3 | Om chatt inkommer som innehåller **känslig - sekretess (gul)** och **Hög Sekretess (Röd)** ska mottagaren genast meddelas att känslig dialog på grund av säkerhetsskäl inte kan hållas per chatt. Hänvisa avsändaren till andra säkra kommunikationskanaler. Svara inte avsändaren eller vidarebefordra ej i samma chattkonversation, utan påbörja känslig dialog i avsedda kommunikationskanaler. Varpå meddelandet ska raderas från chatten. |

Chatt är för en del medarbetare ett vanligt och viktigt sätt att kommunicera internt inom kommunen och till vissa grupper av externa parter. Det är dock viktigt att tänka på att kommunikation med chatt normalt är helt öppen. Att sända chatt kan jämföras med att skicka vykort.

## A5. Lagring och säkerhetskopiering

**Riktlinjer för lagring och säkerhetskopiering**

| | |
|---|---|
| A 5.1 | Kommunens information ska lagras i kommunens tillhandahållna tjänster på så sätt att den finns tillgänglig för den som behöver den. |
| A 5.2 | Om information i undantagsfall behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket eller till din OneDrive kopplat till ditt kommunkonto. Om hårddisken på din dator kraschar kommer annars informationen att vara förlorad. |
| A 5.3 | Om information på nätverket eller i din OneDrive har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, kontrollera först om dokumenten finns kvar i papperskorgen, vilket det normalt sett bör göra. Om inte så ska Servicedesk kontaktas. |

| | |
|---|---|
| A 5.4 | **Känslig-Sekretess (Gul)** information ska i första hand lagras i verksamhetssystem. |
| A 5.5 | **Känslig-Sekretess (Gul)** information får endast lagras i avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan. |
| A 5.6 | **Hög Sekretess (Röd)** information ska endast hanteras i verksamhetssystem om verksamhetssystemet har en tydlig funktion för sekretessmarkering. Saknar verksamhetssystemet stöd för detta får inte verksamhetssystemet hantera skyddade personuppgifter. Uppgifterna måste då vara fiktiva alternativt strikt hanteras utanför den digitala miljön. |
| A 5.7 | Lokal lagring (synkronisering) av **Känslig – Sekretess (Gul)** information, t.ex. på en persondator, får endast ske på en kommunägd dator. |
| A 5.8 | Lagring av **Känslig – Sekretess (Gul)** information på ett USB minne tillåts endast om informationen är rätt klassat och USB minnet är krypterat med krypteringsteknik som Söderhamns kommun tillhandahåller. Kontakta servicedesk. USB minnet ska förvaras betryggande då det inte används. |
| A 5.9 | Fysiska dokument som innehåller **Hög – Sekretess (Röd)** information ska förvaras inlåsta på så sätt att uppgifterna endast är tillgängliga för den personal som behöver dem. |

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 5.10 | Endast godkända molntjänster är tillåtna att användas. Du ansvarar för att kontrollera vilka molntjänster som är tillåtna inom din verksamhet |
| A 5.11 | Som användare ska du inte koppla en molntjänst du använder privat till din kommunala e-postadress. |
| A 5.12 | Söderhamns kommuns information får inte lagras i personliga molntjänster (Dropbox mfl). |
| A 5.13 | **Hög Sekretess (Röd)** information får inte lagras i molntjänster |

**Riktlinjer för lagring i OneDrive/Teams**

| | |
|---|---|
| A 5.14 | Du ansvarar för att allmänna handlingar tas om hand för registrering och arkivering, och att information i din OneDrive gallras enligt fastställda informationshanteringsplaner. |
| A 5.15 | **Känslig Sekretess (Gul)** och **Hög Sekretess (Röd)** information får inte lagras i OneDrive eller Teams av juridiska skäl. På OneDrive sparar du annat material som du lätt vill komma åt att redigera när som helst, var som helst. Det är i OneDrive du har dina egna arbetsrelaterade dokument. Via OneDrive kan du dela ett dokument med en eller ett par kollegor om du behöver synpunkter eller dialog kring ett innehåll. |

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror. Office 365 är exempel på molntjänster som Söderhamns kommun valt att införa.

## A6. Mobila enheter

**Riktlinjer för hantering av mobila enheter**

| | |
|---|---|
| A 6.1 | Känslig och sekretessinformation måste vara krypterad på mobila enheter. |
| A 6.2 | Mobila enheter ska låsas med lösenord eller liknande. |
| A 6.3 | Mobila enheter som tillhandahålls av Söderhamns kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera. |
| A 6.4 | Uppsatta säkerhetsinställningar i enheter får inte ändras. |
| A 6.5 | Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din närmaste chef. |
| A 6.6 | 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 6.7 | Privat utrustning kan anslutas till kommunens gästnät. |
| A 6.8 | Kommunenheter får enbart anslutas till trådlösa nätverk som är betrodda och lösenordskyddade. Säkerhetsklassad information Känslig – Sekretess (Gul) och Hög sekretess (Röd) får ej anslutas till ”öppna” nät till exempel på hotell, caféer, tåg eller flygplan. |
| A 6.9 | Vid distansarbete måste kommunens utrustning användas för kommunens information. |

**Riktlinjer för fysisk hantering av mobila enheter**

| | |
|---|---|
| A 6.10 | Försiktighet ska iakttas vid mobilt arbete i publika miljöer, exempelvis kan skärmen på enheten skyddas med insynsskydd (s.k. sekretesskydd). |
| A 6.11 | Arbete med Känslig – Sekretess (Gul) och Hög sekretess (Röd) information får inte ske i publika miljöer. Om man som anställd behöver behandla känslig information i publika rum som till exempel bibliotek är det viktigt att göra det på ett sådant sätt att risken för att känslig information sprids till obehöriga elimineras. |
| A 6.12 | Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme. |
| A 6.13 | Förlust av enhet ska omedelbart anmälas till Servicedesk, detta ska göras innan polisanmälan. I många fall finns möjligheter att fjärradera information. |
| A 6.14 | Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns. Kommunen tillåter inte att medarbetare friköper sina mobila enheter vid avslut av anställning. |
| A 6.15 | Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt. |
| A 6.16 | Vid service ska den mobila enheten inlämnas enligt fastställda rutiner, dessa finner du på intranätet. |

| | |
|---|---|
| A 6.17 | Om utrustningen måste lämnas in för service så ska du försäkra dig om att den inte innehåller **känslig eller sekretessinformation.** |

Den IT-utrustning som tillhandahålls av Söderhamns kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Mobila enheter 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.

Särskilda regler för smarta telefoner och surfplattor

**Regler för smarta telefoner och surfplattor**

| | |
|---|---|
| A 6.18 | Söderhamns kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som tillhandahålls för arbetet och även till den arbetsrelaterade informationen som finns i dessa enheter. Enligt offentlighetsprincipen kan det också vara möjligt för allmänheten att begära ut allmänna handlingar, till exempel arbetsrelaterade SMS eller bilder, som förvaras på telefonen/surfplattan. |
| A 6.19 | Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. |
| A 6.20 | Pinkod (6 siffror), fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 000000, 123456 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till betalkort. Du får inte skriva upp koden på telefonen eller surfplattan. |
| A 6.21 | Vårda utrustningen och använd exempelvis skärmskydd och skal. |
| A 6.22 | Huvudregeln är att vid anställningens upphörande ska surfplatta och den smarta telefonen återlämnas till närmaste chef. |
| A 6.23 | Vid längre tjänstledighet kan telefonen behöva lämnas åter, det avgör närmaste chef. |
| A 6.2 | En smart telefon är ett viktigt verktyg för säker inloggning till kommunens IT-resurser som kräver multifaktorinloggning – därför måste din smarta telefon som arbetsgivaren tillhandahållit hanteras som en värdehandling. |

## A7. Skadlig kod

**Riktlinjer för skydd mot skadlig kod**

| | |
|---|---|
| A 7.1 | Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod. |
| A 7.2 | Anslut endast arbetsrelaterad IT-utrustning till kommunens administrativa nätverk. |
| A 7.3 | Var misstänksam och undvik att klicka på konstiga länkar eller fylla i kontouppgifter. |
| A 7.4 | Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Är du osäker, ring avsändaren och fråga. |
| A 7.5 | Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, gör så här: 1) koppla ifrån wifi/dra ur |

| | |
|---|---|
| | nätverkskabeln 2) låt datorn vara på 3) kontakta Servicedesk. OBS! Anmälan till Servicedesk ska ske per telefon eller besök, inte via e-post. |

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:

- Ett ökande problem är s k Ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma för att få tillbaka åtkomsten till filerna
- Vissa trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare.
- Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap. Exempelvis med syfte att lagra olaglig information

**Spridning av skadlig kod**
Skadlig kod kan spridas till din dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier. Avsändare till e-post kan fejkas och webbsidor är inte alltid de som de utger sig för att vara. Identiteter kan kapas, till exempel på Facebook, och e-postadresser kan fejkas i syfte att lura mottagaren att klicka på länkar.

Vid s k Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt.

IT-utrustning som drabbats av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada. Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

## A8. Internet och sociala media

**Riktlinjer för internetanvändning**

| | |
|---|---|
| A 8.1 | Internet är i arbetet på Söderhamns kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen. |
| A 8.2 | Det är tillåtet att använda Internet för privat bruk om det inte inkräktar på arbetet eller medför kostnader för kommunen. Kommunen förutsätter att den som surfar på Internet endast besöker lagliga webbplatser. |
| A 8.3 | Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Söderhamns kommuns nätverk. |
| A 8.4 | Hemsidor med exempelvis rasistiskt, våldsinriktat eller sexuellt innehåll får inte besökas. Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.<br>. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning etcetera) eller har anknytning till kriminell verksamhet. |
| A 8.5 | De regler som gäller i samhället i övrigt gäller självklart även inom Söderhamns kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt lagar som reglerar personuppgiftsbehandling är exempel på lagar som ibland måste beaktas när man använder Internet. |
| A 8.6 | För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren. |
| A 8.7 | Internet är ett öppet nätverk och endast öppen information får publiceras, alltså inte Känslig - Sekretess (gul) eller Hög Sekretess (röd) information. |

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 A7 finns här särskilda regler för användning av Internet och sociala medier.

Etiska riktlinjer

| | |
|---|---|
| A 8.8 | All kommunikation på Internet från Söderhamns kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte, eftersom kommunens enheter lämnar spår på Internet som leder tillbaka till vår organisation. |
| A 8.9 | Publicera inte något på Internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt samt finns kvar under lång tid. Tänk därför igenom innehållet noga innan du publicerar. |

Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstemannen som utför aktiviteten, och även för Söderhamns kommun som organisation. Det är därför särskilt viktigt att som

representant för Söderhamns kommun beakta god etik och gott omdöme på Internet. Söderhamns kommuns etiska regler och värderingar ska följas.

**Riktlinjer vid användning av sociala medier**

| | |
|---|---|
| A 8.10 | Vid användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Söderhamns kommuns. |
| A 8.11 | Det är viktigt att du skiljer på vad du gör i sociala medier som privatperson och som representant för Söderhamns kommuns verksamheter. |
| A 8.12 | Du har självklart rätt att diskutera Söderhamns kommun och jobbrelaterade saker som privatperson i sociala medier (förutom ärenden som omfattas av sekretess, se nedan). Ibland kan du behöva vara extra tydlig och förklara i vilken roll du uttalar dig eftersom du kan förknippas med din yrkesroll även på fritiden. |
| A 8.13 | Hemliga uppgifter får inte spridas och ärenden som berörs av sekretess eller tystnadsplikt får aldrig avhandlas i sociala medier, varken i privata konton, direktmeddelanden eller som inlägg i kommunens kanaler. |
| A 8.14 | Gör du inlägg eller kommenterar med Söderhamns kommuns profil/användare så representerar du Söderhamns kommun. Skriver du med ditt eget namn och profil som avsändare gör du det som privatperson. |
| A 8.15 | I ditt personliga konto får du inte använda bilder och filmer som tillhör Söderhamns kommun utan att fråga fotografen först. |

Söderhamns kommun är aktivt på sociala medier. Den personal som är utsedda att skriva i kommunens namn har särskilda regler och kunskap om kommunikation. Se vidare Söderhamns kommuns riktlinjer för sociala medier. (Finns att läsa på kommunens intranät)

## A9. Spårbarhet och loggning

**Riktlinjer vid granskning av loggar**

| | |
|---|---|
| A 9.1 | Materialet får inte användas av arbetsgivaren i allmänt kontrollerande syfte. |
| A 9.2 | Misstanke om överträdelse ska vara väl dokumenterat. Dokumentationen ska innehålla beskrivning av händelsen, namn på person eller personer som gjort iakttagelser, datum, tidpunkt etc. Det är en förutsättning för att loggning skall kunna genomföras. Avsaknad av dokumentation innebär att loggning av enskild person inte får slås på. |

**Rutin vid fördjupad granskning**

Om det finns behov av fördjupad granskning av uppgifter på individnivå gäller följande:

**Riktlinjer vid fördjupad granskning**

| | |
|---|---|
| A 9.3 | Vid granskningen skall alltid två personer närvara. |
| A 9.4 | Verksamhetschef utser person från verksamheten och IT-driftchef utser teknisk assistans. Personerna får endast tillgång till loggarna i samband med granskningen. |

| | |
|---|---|
| A 9.5 | Granskningen ska genomföras skyndsamt och enligt fastställd teknisk rutin. |
| A 9.6 | Granskarna skall noggrant dokumentera anledningen till granskningen. I dokumentation skall det framgå vilka som genomfört den, samt datum, tid och plats för granskningstillfället. |

**Gallring av loggar från granskning**
**Riktlinjer av loggar från granskning**

| | |
|---|---|
| A 9.7 | Granskningsloggar ska raderas efter ärendet är avslutat. |
| A 9.8 | Undantag ska göras för loggar som påvisat brottslig aktivitet eller brott mot regler samt loggar som berörs av påbörjad undersökning. |
| A 9.9 | Sådan undersökning innebär att det material som då finns tillgängligt sparas och är tillgängligt till dess att undersökningen avslutats. |

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. Loggning sker i kommunens datorer och nätverk. Loggningen är förenligt med GDPR. Loggarna används även för felsökning. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. Söderhamns kommun kan, 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.

**Pornografi**
Enligt detta styrdokument, som upprättats med stöd av kommunens informationssäkerhetspolicy, är det inte tillåtet att titta eller lyssna på material av pornografisk karaktär. Enligt brottsbalken är innehav av barnpornografi straffbart (brottsbalken 16:10a).
**Anonymitetsservrar**
Innebär att användaren loggar in på en särskild server som erbjuder tjänsten anonymitet. Där kan användaren surfa runt på Internet utan att lämna några spår efter sig. Det som kan spåras är anonymitetsserverns IP-adress.
**Illegal fildelning**
Upphovsrätten innebär att den som skapat ett litterärt eller konstnärligt verk också har rätt till det. I den rätten ingår också att förfoga över verket genom att framställa exemplar av det och att göra det tillgängligt för allmänheten. Enligt upphovsrättslagen är det straffbart att dela ut den informationen till andra genom till exempel illegal fildelning. Förutom det personliga ansvaret riskerar den som medverkat till fildelning att bli skadeståndsskyldig till den som har upphovsrätt.
**Rutin för loggning**
GDPR medger rätt för arbetsgivaren, pga. allmänt intresse, att logga internettrafik utan personligt samtycke, med stöd av informationssäkerhetspolicy och för att säkerställa verksamhetens kontinuitet genom begränsande av internetanvändning för fildelning, kränkning/mobbning, rasism eller barnporr. Materialet får användas för att på ett strukturerat sätt beställa rapport på övergripande nivå (inte personrelaterad) där förbjudna sidor

och på förhand definierade undersökningsområden fastställts. Sådana områden skall vara kända av personalen. Om det ur materialet kan påvisas att det skett slagningar mot förbjudna sidor eller frekvent användning på ett otillbörligt sätt kan verksamhetschef beställa fördjupad granskning av materialet.

**Individuell loggning**

Om det finns misstanke om överträdelse av regler eller misstanke om brottslighet kan verksamhetschef besluta om loggning av enskild persons användning av Internet eller internetanvändning för en grupp användare. Det innebär att samtliga lyckade internetsökningar loggas. Sparade loggar omfattar uppgift om vilken person som besökt adresserna.

**Granskning av loggar**

Direkt granskning av loggar får endast ske när det finns anledning misstänka att överträdelser sker.

## A10. Säkert beteende

**Riktlinjer för muntlig information**

| | |
|---|---|
| A 10.1 | **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** 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, t.ex. 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 10.2 | **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information får överhuvudtaget inte kommuniceras muntligt i publika lokaler. Om man behöver behandla känslig information i kontakten med brukare i publika rum som till exempel bibliotek är det viktigt att föra samtalet på ett sådant sätt att risken för att känslig information sprids till obehöriga minimeras. |
| A 10.3 | Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön. |

| | |
|---|---|
| A 10.4 | Skriftligt material som innehåller **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i egen hurts eller eget skåp när man lämnar arbetsplatsen, även för kortare stunder. |
| A 10.5 | **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett s k smart kort till datorn (SITHS el likn) ska detta tas ut då man lämnar arbetsplatsen. |
| A 10.6 | **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information ska skyddas från insyn med hjälp av sekretessfilter på datorskärm i de fall då sådan information hanteras på plats där insyn från sidan kan ske. Sekretessfilter kan efter bedömning av närmaste chef tillhandahållas av arbetsgivaren |

| | |
|---|---|
| A 10.7 | Besökare får inte vistas utan uppsikt i lokaler där **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta. Datorer i publika rum, till exempel bibliotek, med känslig information får inte lämnas utan uppsikt utan att låsas ner. |
| A 10.8 | Vid fysisk posttjänst ska dubbla förslutna brev (internpostkuvert och kuvert) användas för intern information och rekommenderade försändelser ska användas om externbrev innehåller **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information. |
| A 10.9 | Fax är ett väldigt osäkert kommunikationssätt. Därför håller kommunen på att ersätta faxen med Säker Digital Kommunikation, lösningen ska införas under 2023. Om **Känslig – Sekretess (Gul)** 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 10.10 | Fax får inte användas till Hög Sekretess (Röd) information. |
| A 10.11 | Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information måste så kallad Follow-me printing (inloggning med passerkort) användas. Utskriften ska alltid övervakas så att man är säker på att ingen obehörig kan läsa informationen. Det ska också säkerställas att samtliga dokument är helt utskrivna innan man lämnar skrivaren. |
| A 10.12 | Pappersdokument som innehåller **Känslig – Sekretess (Gul)** och **Hög Sekretess (Röd)** information måste vid kassering strimlas eller kastas i godkända säkerhetskärl. |

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 **Känslig – Sekretess (Gul)** eller **Hög sekretess (Röd)** 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 till exempel omdömen om chefer och medarbetare – skvaller, rykten m m – eller information om en oförutsedd händelse, t.ex. ett brott. Sådan information kan vara känslig och är i så fall att betrakta som **Känslig – Sekretess (Gul)** information.

# Kapitel B – Styrning av informationssäkerhet

**Innehåll Kapitel B**



## Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Söderhamns kommun. Det beskriver också hur ansvarsfördelningen ser ut i stort. Ansvar för varje målgrupp återfinns också i varje kapitel, varför den övergripande ansvarsfördelningen i detta kapitel i huvudsak är informativ och ger en överblick över ansvaret för informationssäkerhet.

Den primära målgruppen för detta kapitel är de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i systemförvaltning, projekt, processer eller andra verksamheter. Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Söderhamns kommun, exempelvis sådana som arbetar med ledning och styrning av andra närliggande områden och processer som exempelvis kvalitet och annan säkerhet.

I kapitlet ges en introduktion till informationsklassning och den modell för informationsklassning som Söderhamns kommun antagit i och med dessa riktlinjer.

## B1. Roller, ansvar och organisation

*Grundprincip*

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till medarbetare, verksamheter och kommunens ledning att kunna ta ansvaret för informationssäkerheten.

*Övergripande ansvar*

Kommunstyrelsen har det yttersta ansvaret för kommunkoncernens informationssäkerhet. Kommunstyrelsen fastställer övergripande mål och

inriktning för informationssäkerhet genom en kommunövergripande informationssäkerhetspolicy.

Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunstyrelsen fastställda informationssäkerhetspolicyn. Kommundirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande riktlinjer för informationssäkerhet.

Ledningen ansvarar för att alla medarbetare i Söderhamns kommun efterlever informationssäkerhetspolicyn och riktlinjer för informationssäkerhet. Ledningen bör visa sitt stöd för dessa dokument och fungera som förebild.

*Ansvar inom respektive verksamhet*
Varje nämnd är ansvarig för informationssäkerheten inom sitt verksamhetsområde. Nämnd kan vid behov besluta om instruktioner som kompletterar de centrala riktlinjerna förinformationssäkerhet.

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger varje verksamhetsansvarig att se till att sina medarbetare efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig informationssäkerhet i verksamheten kan uppnås.

Säkerhetsansvaret i sig kan inte delegeras, däremot kan ansvaret att genomföra vissa arbetsuppgifter fördelas.

*Medarbetares ansvar*
Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler. Varje anställd har även skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon enskild befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande.

➔ Riktlinjer för medarbetare återfinns i Kapitel A

*Personuppgiftsansvar*
Kommunstyrelsen och övriga nämnder är personuppgiftsansvariga inom respektive verksamhetsområde och ska utse personuppgiftsombud. Som personuppgiftsansvariga har de det yttersta ansvaret för all behandling av personuppgifter inom sitt verksamhetsområde även om den personuppgiftsansvarige har utsett ett personuppgiftsombud. Om behandlingen sker i strid med personuppgiftslagen eller andra bestämmelser kan den personuppgiftsansvarige ställas till ansvar, oavsett om denne haft uppsåt att handla i strid med lagen eller varit oaktsam.

Under år 2018 trädde EU:s nya dataskyddsförordning i kraft. Den ställer nya krav på kommunens hantering av personuppgifter.

*Centralarkivet (Arkivmyndigheten i Söderhamns kommun)*
Arkivmyndighetens uppgifter framgår av 3 § i kommunfullmäktiges antagna föreskrifter om arkivvård. Syftet med uppgifterna är att arkivmyndigheten ska bidra till att säkerställa att övriga arkivbildande myndigheter följer arkiv- och offentlighetslagstiftningens krav på hanteringen av allmänna handlingar.

Hos arkivmyndigheten finns ett centralarkiv som innehåller de arkiv som övertagits enligt överenskommelse eller till följd av lag. Centralarkivet består av ett analogt arkiv samt ett e-arkiv.

Centralarkivet ska vårda hos sig förvarat arkivbestånd samt tillhandahålla och främja arkivens tillgänglighet och användning i kulturell verksamhet, forskning och i det löpande sektorsarbetet samt verka för att arkiven ska bli fullständiga.

Mer information finns i Söderhamns kommuns riktlinjer om arkivvård.

*Systemägares ansvar*
Systemägaren ansvarar för att systemen efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om systemets informationssäkerhetsnivåer genom att klassning sker i enlighet med SKR:s modell för informationsklassning Klassa 3.0. Informationssäkerhetsansvar hos övriga roller inom förvaltningsorganisationen beskrivs i Kapitel C.

I den mån det inte finns utpekade systemägare för ett system, följer ansvaret verksamhetsansvaret.

➔ Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning återfinns i Kapitel C

*Ansvar i projekt*
Verksamheten äger projektet via en utsedd projektägare som säkerställer att säkerhetsfrågorna beaktas. Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägaren fastställa säkerhetsnivån för det som utvecklas. Under projektets gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna. Projektledaren ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

*Digitaliseringsavdelningens ansvar*
Digitaliseringsavdelningen ansvarar för att säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

*IT-säkerhetsansvarig*
Det ska finnas en utpekad IT-säkerhetsansvarig som samordnar arbetet med säkerheten i Söderhamns kommuns IT-miljö och som är stödjande vid kravställning på externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i Kapitel D.

➔ Riktlinjer för informationssäkerhet i IT-miljön återfinns i Kapitel D

*Informationssäkerhetsansvarig*
Informationssäkerhetsarbetet i kommunen leds och samordnas av en informationssäkerhetsansvarig.

På delegation av kommundirektören beslutar informationssäkerhetsansvarig om godkännande av undantag i Riktlinjer för informationssäkerhet i samråd med berörda samt kommunens säkerhetschef.

Informationssäkerhetsansvarig ansvarar för:
- att kommunens styrande dokument inom området är aktuella, som informationssäkerhetspolicy och riktlinjer för informationssäkerhet,
- att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet,
- kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom kommunen, t.ex. genom rådgivning och utbildning,
- att stödja verksamheterna i frågor som rör informationssäkerhet,
- kontroll och uppföljning av informationssäkerheten,
- omvärldsbevakning inom informationssäkerhetsområdet,
- leda kommunens Digitaliseringsråd (se nedan).

*Digitaliseringsrådet*
Digitaliseringsrådet leds av informationssäkerhetsansvarige som utser övriga ledamöter efter samråd med verksamhetschef. Digitaliseringsrådet ska sammanträda ca 20 gånger per år och har uppgift och befogenheter att:
- bereda och registrera ärenden som gäller undantag från kommunens Riktlinjer för informationssäkerhet (godkännes av informationssäkerhetsansvarige i samråd med berörda samt kommunens säkerhetschef),
- bereda dokument, t.ex. styrande dokument, metoder och vägledningar,
- fungera som remissinstans och rådgivare i relaterade frågor,
- vara ett forum för erfarenhetsutbyte och omvärldsbevakning,

*Kommunens revisorer*
Kommunens revisorer utför kontroll av informationssäkerheten inom ramen för ordinarie revisioner.

## B2. Dokumentstruktur

Det är fem dokument som är centrala för kommunens arbete med informationssäkerhet:

*Informationssäkerhetspolicy*
- Riktlinjer för informationssäkerhet (detta dokument)
- Riktlinjer för digital lagring
- Säkerhetsinstruktion för IT-användare

Sektorvisa handlingsplaner digital verksamhetsutveckling

Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet (detta dokument) riktar sig till alla medarbetare inom Söderhamns kommun:
- Informationssäkerhetspolicyn är ett övergripande dokument som uttrycker ledningens viljeinriktning med informationssäkerhet. Beslutas av Kommunfullmäktige och uppdateras vid behov.
- Riktlinjer för informationssäkerhet innehåller regler för hantering av information. Riktlinjerna är uppdelade i kapitel för olika målgrupper. Beslutas av kommunstyrelsen och uppdateras vid behov.
- Riktlinjer för digital lagring är ett stöd för anställda vart man lagrar egen information och övergripande informationshantering.
- Sektorvisa handlingsplaner för digital verksamhetsutveckling är en plan för sektorns verksamhetsutveckling med digitala verktyg och tjänster.

Modeller, metoder, vägledningar och andra stöddokument kan tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet. Lokalt, t.ex. i sektorer och för digitaliseringsrådet, kan mer specifika instruktioner och vägledningar tas fram i syfte att komplettera eller förtydliga riktlinjerna för informationssäkerhet.

**Riktlinjer för dokumentstruktur för informationssäkerhet**

| | |
|---|---|
| B.2.1 | Söderhamns kommuns informationssäkerhet och dess behov ska analyseras i en informationssäkerhetsanalys. Analysen ska genomföras minst vart fjärde år och ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av övriga styrande dokument. |
| B.2.2 | Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser. |
| B.2.3 | Det ska finnas en för Söderhamns kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet. |
| B.2.4 | Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som konkretiserar informationssäkerhetspolicyn och som riktar sig till relevanta målgrupper. |
| B.2.5 | Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetpolicyn och riktlinjerna för informationssäkerhet. |

## B3. Informationsklassning

Informationsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för, och kan

styra vilket skydd som krävs för olika informationsmängder. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd – med onödigt höga kostnader som följd. Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Söderhamns kommuns verksamheter.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet och tillgänglighet är en fundamental aktivitet i ett ledningssystem för informationssäkerhet (LIS) och ett krav i standarden SS-ISO/IEC 27001. Det är också en rekommendation från SKR och MSB – Myndigheten för samhällsskydd och beredskap – att organisationer ska klassa sin information och bygga sina säkerhetsåtgärder utifrån Klassa 4.0. Se även Kap A1 som beskriver informationsklassning i ett övergripande perspektiv.

| Risk klass | Risknivå | Nivå där risk får accepteras | Krav på behandling | Krav på information | Dokumentation i riskregister |
|---|---|---|---|---|---|
| Högs sekretess (Röd) | Extremt hög risk | Högsta ledningen | Omedelbart | Högsta ledningen och säkerhetsledning | Centralt och riskägarens dokumentation |
| Känslig – sekretess (Gul) | Hög risk | Verksamhetschef | Inom 3 mån | Säkerhetsansvarig och verksamhetschef | Centralt och riskägarens dokumentation |
| Begränsad (Grön) | Medelhög risk | Enhetschef | Inom 12 mån | Enhetschef | Centralt och riskägarens dokumentation |
| Öppen (Vit) | Låg risk | Riskägare | Inga krav | Inga krav | Endast risk-ägarens eget |

*Klassa 4.0 risknivåer*

*Söderhamns kommuns modell för informationsklassning*
Öppen information behöver alltså inte ha något skydd mot insyn och har normalt ingen begränsad åtkomst. Däremot är det viktigt att förstå att all information – även öppen – har minst normala skyddskrav när det gäller dess riktighet och tillgänglighet. Det kan också krävas beslut för att viss information ska vara öppen och publik.

Idén med informationsklassning är att skydd ska anpassas till kraven på en viss informationsmängds konfidentialitet, riktighet, tillgänglighet och spårbarhet. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet.

*Vad ska klassificeras?*
Det är informationen som är den primära tillgången och som ska klassas, och som sedan styr vilka skyddsåtgärder de olika nivåerna av skyddskrav medför. Resurser som används för att hantera informationen, t.ex. programvaror, tjänster och fysiska tillgångar, ska utformas och anpassas till de krav som klassningen i förlängningen ställer på dessa.

IT-system ska klassas på grundval hur informationen är klassad som finns i eller hanteras av systemen. En viktig uppgift för objektägare och förvaltningsledare är därför att klassa sina system så att rätt skyddskrav erhålls. Riktlinjer för detta finns i Kapitel C.

➔ Kapitel C – Riktlinjer för informationssäkerhet i verksamhetsnära förvaltning.

Informationsklassning har nyligen påbörjats i Söderhamns kommun, och långt ifrån all information är klassad. Målsättningen är främst att kritisk information ska klassas som har **höga skyddskrav** för en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet.

Observera att det finns 2 olika begrepp Klassa, det vi avser ovan är Klassa 4.0 för informationssäkerhetsklassning. Den andra Klassa är Samrådsgruppens klassa 2.1 för att klassificera informationstyper – 2000-talets diarieplan.

*Användningsområden och målgrupper*
Modellen vänder sig dels till de i Söderhamns kommun som är verksamhetsansvariga och/eller ägare av information- och systemägare, och dels till de som ansvarar för att rätt nivå av skydd skapas och upprätthålls. Den klassade informationen utgör ett underlag för en verksamhet vid kravställning av tjänster, exempelvis IT-tjänster, både internt och externt. Klassningsmodellen kan därigenom fungera som ett gemensamt ramverk och kommunikationsmodell vid förhandling mellan beställare och leverantör av tjänster.

Identifiering och klassificering av information bör ske initialt när informationssäkerhetsbehovet ska analyseras men även som ett led i löpande förbättring eller vid förändringar av verksamheter eller IT-system.

För de flesta medarbetare gäller endast aspekten Konfidentialitet, vilket betonas i Kapitel A som riktar sig till alla medarbetare. Figur 2).

| Informationsklass | Behörighet/spridning | Exempel |
|---|---|---|
| 4 Hög Sekretess (Röd) | Endast ett mycket begränsat antal behöriga personer | Skyddade personuppgifter, information som om den hamnar i orätta händer medföra fara för liv och hälsa eller samhällsskada |
| 3 Känslig-Sekretess (Gul) | Endast den som behöver informationen för att klara sin arbetsuppgift, särskild åtkomstbegränsning med god spårbarhet | Känsliga personuppgifter, integritetskänsliga (extra skyddsvärda) såsom personnummer och sociala förhållanden, information under pågående upphandling, skalskyddsritningar |
| 2 Begränsad (Grön) | Normal åtkomstbegräsning med viss spårbarhet | Allmänna personuppgifter, allmänna offentliga handlingar, födelsedata (6 första siffrorna i personnummer YYMMDD) |
| 1 Öppen (Vit) | Ingen åtkomstbegränsning | Handlingar utan direkta eller indirekta personuppgifter |

En mer utförlig vägledning som stöd för informationsklassning finns på www.skr.se.

**Riktlinjer för informationsklassning**

| | |
|---|---|
| B.3.1 | Det ska finnas en för Söderhamns kommun, gemensam modell för informationsklassning. Klassa 4.0 för säkerhetsklassning av information och Klassa 2.1 för informationshantering/diarieplan. |
| B.3.2 | Söderhamn kommuns modell för informationsklassning ska tillämpas för kravställning på informationssäkerhet genom att information ska klassas i enlighet med modellen och krav på säkerhetsåtgärder ska kopplas till de olika nivåerna i klassningsmodellen. |

## B4. Ledningssystem för informationssäkerhet

I Söderhamns kommuns informationssäkerhetspolicy anges att man ska bedriva ett systematiskt informationssäkerhetsarbete som baseras på standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).

Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS.

Eftersom kommunen och dess omvärld är i ständig förändring är informationssäkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa en skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon.

Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

I Söderhamn kommun har arbetet med att skapa ett LIS påbörjats i och med dessa riktlinjer där roller, ansvar och informationsklassning är viktiga element. Att planera och införa ett LIS kommer dock att fortgå under de närmaste åren.

Söderhamn kommuns ledningssystem för informationssäkerhet LIS, ska utgå från standardserien SS-ISO/IEC 27000. Standardserien innefattar en stor mängd standarder, men två standarder kan sägas utgöra seriens huvudstandarder:

- SS-ISO/IEC 27001:2014 – Informationsteknik – Säkerhetstekniker Ledningssystem för informationssäkerhet – krav. Denna standard ställer som namnet antyder krav på ett LIS, dvs. vad det ska innefatta. I standardens bilaga A finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas.
- SS-ISO/IEC 27002:2014 – Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder. Denna standard ger vägledning för införande av säkerhetsåtgärderna i föregående standards bilaga A.

Dessa båda standarder är i Sverige och internationellt dominerande ramverk för styrning av informationssäkerhet. Sedan år 2009 är det exempelvis tvingande för svenska statliga myndigheter att tillämpa dessa enligt MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1, tidigare MSBFS 2009:10).

Standarderna i serien utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet. Utgångspunkten är också att det är information som ska skyddas, utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet, medan IT är sekundära resurser som används för att hantera informationen.

Att standardserien är så etablerad och spridd innebär fördelar. Förutom att man tar tillvara samlade kunskaper och erfarenheter från hela världen så använder man ett gemensamt ramverk och en gemensam terminologi som underlättar vid kommunikation och samverkan med andra aktörer, exempelvis i samband med utbildning, revisioner och upphandlingar.

Det finns även andra standarder i standardserien som framöver kan vara av intresse för Söderhamn kommun, exempelvis för mätning av informationssäkerhet (27004) och hantering av informationssäkerhetsincidenter (27035).

Ett LIS för Söderhamn kommun kommer att planeras och införas under ledning av informationssäkerhetsansvarig med start under år 2024. Detta kommer att omfatta samtliga delar av informationssäkerhetsarbetet i kommunen.

**Riktlinjer för ledningssystem för informationssäkerhet (LIS)**

| | |
|---|---|
| B.4.1 | Söderhamn kommun ska designa och införa ett ledningssystem för informationssäkerhet. |

## B5. Personalsäkerhet

Personal är den viktigaste resursen i kommunen, och det är personal som dagligen hanterar information, manuellt eller med stöd av IT. Många roller kommer i kontakt med och hanterar kritisk och känslig information, och det är därför att av största vikt att personalen får information och utbildning om informationssäkerhet, och att det finns rutiner i samband med anställning, förändring och avslut av anställning.

*Före och i samband med anställning*
Bakgrundskontroll av sökande till tjänster i Söderhamn kommun ska ske genom verifiering av sökandes meritförteckning, t.ex. genom kontakt med referenser och bekräftelse av påstådda akademiska och yrkesmässiga kvalifikationer.

För vissa kritiska tjänster krävs en förstärkt kontrollform av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information.

Lagsstiftningen om registerkontroll för skydd av barn och unga ska självklart efterlevas.

För befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (1996:627), ska det i anställningsförfarandet genomföras en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Söderhamn kommuns säkerhetsskyddsplan. Registerkontrollen administreras av kommunens säkerhetschef.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, t.ex. informationsägarskap. Alla anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal som även ska gälla efter avslut av anställning.

**Riktlinjer för personalsäkerhet före och i samband med anställning**

| | |
|---|---|
| B.5.1 | Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras. |
| B.5.2 | Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. |
| B.5.3 | För befattningar som har betydelse för rikets säkerhet, och som omfattas av Säkerhetsskyddslagen (1996:627) ska det i anställningsförfarandet genomföras en registerkontroll. B.5.4 Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Och annat ansvar som följer med rollen, t.ex. informationsägarskap. |
| B.5.5 | Anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal. |

*Under anställning*
I enlighet med informationssäkerhetspolicyn ska medarbetare inom kommunen ha ett högt medvetande avseende informationssäkerhet.

Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.

Roller som har särskilda uppgifter inom informationssäkerhet, t.ex. inom IT-säkerhet eller förvaltningsorganisationen, ska få lämplig fortbildning inom området som är relevant för respektive befattning. Om anställda bryter mot gällande informationssäkerhetsregler ska dessa ärenden hanteras individuellt av ansvarig chef med stöd från personalavdelningen på samma sätt som vid andra misskötselärenden.

**Riktlinjer för personalsäkerhet under anställning**

| | |
|---|---|
| B.5.6 | Alla medarbetare och i förekommande fall externa aktörer ska erhålla lämplig utbildning för att kunna efterleva kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet. B.5.7 Roller som har särskilda uppgifter inom informationssäkerhet ska får lämplig fortbildning inom området som är relevant för deras befattning. |
| B.5.8 | Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har brutit mot gällande informationssäkerhetsregler. |

*Avslut eller ändring av anställning*
Vid avslut eller ändring av anställning kan ansvar och skyldigheter för informationssäkerhet förbli gällande, exempelvis sekretessavtal och tystnadsplikt om den anställde haft tillgång till konfidentiell information. Detta ska definieras och kommuniceras till den anställde vid anställning/tillträdande av roll och framgå i sekretessavtal.

Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning.

**Riktlinjer för avslut eller ändring av anställning**

| | |
|---|---|
| B.5.9 | Ansvar och skyldigheter för informationssäkerhet som förblir gällande efter avslut eller ändring av anställning ska definieras och kommuniceras vid anställningstillfället eller tillträdande av roll och framgå i sekretessavtal. |
| B.5.10 | Återlämnande av IT-resurser och indrag av åtkomsträttigheter till information och IT-resurser ska ske i direkt samband med avslut eller ändring av anställning. |

## B6. Leverantörsrelationer

Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Söderhamn kommuns modell för informationsklassning. Kravkatalogen ska kunna användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster. En kravkatalog baserad på standarden SS-ISO/IEC 27002:2014 planeras att tas fram under år 2024.

Det ska finnas en vägledning som beskriver hur en kontroll av en IT-tjänst ska genomföras. Den ska kunna användas som stöd inför användandet av en ny tjänst eller vid kontroll av en befintlig tjänst.

Riktlinjer för upphandling av IT-resurser återfinns i avsnitt D7.

Riktlinjer för kontroll av IT-tjänst återfinns i avsnitt C9.

**Riktlinjer för leverantörsrelationer**

| | |
|---|---|
| B.6.1 | Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Söderhamn kommuns modell för informationsklassning. Vägledningen ska kunna användas som stöd vid extern upphandling av IT-tjänster. |
| B.6.2 | Det ska finnas en vägledning för kontroll av IT-tjänst. Syftet med vägledningen ska vara att säkerställa att IT-tjänsten kan skydda verksamheten och dess information under hela dess livscykel. |

## B7. Efterlevnad och granskning

Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet ska följas upp. I praktiken innebär det främst att riktlinjerna för informationssäkerhet granskas och följs upp; att riktlinjerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan. I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-resurser med **höga skyddskrav**.

Granskning och uppföljning av informationssäkerhet, inklusive dess styrning, kommer att utvecklas i och med det ledningssystem för informationssäkerhet (LIS) som ska införas i kommunen då en väsentlig del i ett LIS handlar om efterlevnadskontroll.

Revision av hela eller stora delar av Söderhamn kommuns informationssäkerhet ska göras minst vartannat år.

Granskning av efterlevnad av informationssäkerhet bör också genomföras av extern part, exempelvis på uppdrag av Kommunrevisionen.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.

Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Detta regleras av riktlinjer i Kapitel D – Informationssäkerhet i IT-miljön (avsnitt D10).

**Riktlinjer för efterlevnad och granskning av informationssäkerhet**

| | |
|---|---|
| B.7.1 | Efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet ska följas upp. |
| B.7.2 | Söderhamns kommuns informationssäkerhet ska utsättas för oberoende granskning. |

# Kapitel C: Informationssäkerhet i verksamhetsnära förvaltning

**Innehåll Kapitel C**



## Inledning

Söderhamns kommun har beslutat att tillämpa en modell för Systemförvaltning. Det här kapitlet kompletterar de riktlinjerna med särskilda riktlinjer rörande informationssäkerhet i den verksamhetsnära förvaltningen och riktar sig främst till roller i denna.

I Kapitel D som riktar sig till Söderhamn Näras IT-drift och där återfinns informationssäkerhetsrelaterade riktlinjer för deras verksamhet. Om man för ett system eller en systemgrupp ännu inte har börjat tillämpa systemförvaltningsmodellen så ska det ändå finnas en utsedd ägare för det aktuella systemet och som då ansvarar för säkerheten i systemet. De riktlinjer som finns i detta kapitel gäller även för dessa.

## Roller och ansvar

Nedan beskrivs ansvar rörande informationssäkerhet för rollerna i den verksamhetsnära förvaltningen. Motsvarande ansvar för de IT-nära rollerna återfinns i Kapitel D – informationssäkerhet i IT-miljön. Som nämnts ovan är dessa ansvar tillägg till generella ansvar enligt systemförvaltningsmodellen.

*Systemägare*
I enlighet med Söderhamns kommuns informationssäkerhetspolicy är systemägare ansvarig för systemens informationssäkerhet. Systemägaren ska besluta om systemets informationssäkerhetsnivåer genom att klassning sker i enlighet med Söderhamns kommuns modell för informationsklassning. Systemägaren ska tilldela tillräckligt med resurser i systemets förvaltningsplaner så att informationssäkerhetsnivån kan uppnås.

*Sektorsamordnare*
Sektorsamordnare leder systemförvaltningsarbetet inom sektorn och i det ansvaret ingår att system eller grupper av system klassas så att rätt skyddsnivåer

uppnås, och att informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs. Sektorsamordnare kan vid behov delegera arbetsuppgifter till systemförvaltare och systemspecialister.

*Informationsägare*
En informationsägare är den som har ansvar för en viss informationsmängd. Informationsägaren ska avgöra hur informationen ska klassas och utifrån denna ställa krav på hur information kan och får hanteras och användas.

Om ett system har en homogen mängd information som kan kopplas till den verksamhet som en systemägare ansvarar för, är normalt systemägaren även informationsägare. I de fall systemägaren inte också är informationsägare för informationen i objektet (t.ex. ett diariesystem som hanterar många olika slag av information), så är informationsägare istället kravställare på systemägaren vad gäller säkerheten för den aktuella informationen.

## C1. Dokumentation av informationssäkerhet

Informationssäkerhet ska vara en naturlig del i förvaltningen av system och de system som ingår i verksamheten. Säkerhetsförhållanden ska vara dokumenterade i systemsäkerhetsbeskrivningar och planerade säkerhetsåtgärder ska ingå i förvaltningsplanerna så att de formellt fastställs av systemägaren och har en budget.

Informationsrelaterade mål och åtgärder ska finnas med i systemets förvaltningsplaner. Mål och åtgärder kan uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

**Informationssäkerhet i förvaltningsplaner**

| | |
|---|---|
| C.1.1 | Informationsrelaterade mål och åtgärder ska finnas med i objekts förvaltningsplaner. |

*Systemsäkerhetsbeskrivning*
Systemets säkerhetsförhållanden ska dokumenteras systemsäkerhetsbeskrivningar. En systemsäkerhetsbeskrivning ska finnas för varje system. Av systemsäkerhetsbeskrivningen ska det framgå:

- Vilka informationsmängder som hanteras i systemet och hur dessa är klassade (se avsnitt C2)
- Hur systemet är klassat (se avsnitt C2)
- Hur behörighetshantering och loggning går till (se avsnitt C3)
- Hur ändringshantering går till (se avsnitt C4)
- Användarinstruktioner med inriktning på säkerhet (se avsnitt C5)
- Planerade och genomförda riskanalyser och resultat från dessa (se avsnitt C6)
- Hur incidenthantering går till och vilka incidenter som har inträffat med referenser till incidentrapporter (se avsnitt C7)
- Vilken kontinuitetshantering som finns (se avsnitt C8)

**Systemsäkerhetsbeskrivning**

| | |
|---|---|
| C.1.2 | System ska ha en systemsäkerhetsbeskrivning där systemets informationssäkerhet är dokumenterad. |

## C2. Informationsklassning och systemklassning

Informationsklassning innebär att information klassas i olika nivåer utifrån dess skyddskrav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk information så att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd med höga kostnader som följd.

System ska också klassas och den klassningen ska baseras på hur den ingående informationen är klassad. Klassning av information och system ska ske i enlighet med Söderhamns kommuns modell för informationsklassning som beskrivs i Kapitel B.

Informationsklassning ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Söderhamns kommuns verksamheter.

Frågor man ska ställa sig när man klassar är:

- Vilka konsekvenser blir det om informationen läcker till obehöriga (konfidentialitet)?
- Vilka konsekvenser blir det om informationen är felaktig eller inaktuell (riktighet)?
- Vilka konsekvenser blir det om (behöriga) inte får tillgång till informationen (tillgänglighet)?

När man klassar en informationsmängd enligt modellen ska den bedömas utifrån alla tre aspekter och får då en viss klassningsprofil. En viss informationsmängd kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet.

Klassning av ett system ska baseras på klassningen av den information som systemet hanterar. Ett system kan lägst ge den klassning som den information som den ingående informationen har.

Om ett system innehåller många olika mängder information som ännu inte är klassad kan man behöva göra preliminär klassning av systemet tills all informationsklassning är gjord. Om man vet att det finns höga skyddskrav för någon informationsmängd i någon aspekt så får systemet automatiskt höga skyddskrav för denna aspekt. Vid osäkerhet är det bättre att ”överklassa” än att ”underklassa”.

**Det viktiga är att kritisk information, dvs. information med höga skyddskrav i någon av de tre aspekterna, är identifierad och klassad därefter så att tillräckligt skydd kan skapas för systemet.**

Hur system klassats utgör ett underlag vid kommunikation och kravställning mot Söderhamns kommuns IT-leverantör eller mot externa leverantörer. Kapitel D riktar sig mot Söderhamn Näras IT-drift och där finns särskilda säkerhetsåtgärder för system med **höga skyddskrav.**

Klassningen av system ger också ett underlag för hur användare kan och får arbeta i system. I Kapitel A som riktar sig till samtliga medarbetare finns en mängd hanteringsregler som i vissa fall skiljer sig beroende på hur information är klassad.

Särskilda rutiner och regler ska upprättas för hantering av konfidentiell information, som exempelvis skyddade personuppgifter. Sådana rutiner och regler ska finnas med i användarinstruktioner (se avsnitt C5).

**Riktlinjer för klassning av förvaltningsobjekt**

| | |
|---|---|
| C.2.1 | Kritiska informationsmängder i system ska vara inventerad och klassad enligt Söderhamns kommuns modell för informationsklassning. |
| C.2.2 | System ska klassas som helhet baserat på den klassning som är gjord av kritisk information i systemet. |
| C.2.3 | Särskilda rutiner och regler för ett system ska upprättas för hantering av konfidentiell information, som exempelvis skyddade personuppgifter. |

## C3. Behörighetshantering och loggning

Behörigheter innebär vissa rättigheter att använda en informationstillgång, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användar-ID och lösenord. Ju känsligare information som bearbetas, desto högre är kravet på skydd mot obehörig åtkomst.

Grundprincipen för behörighet ska baseras på vilken information användare behöver för att kunna utföra sina arbetsuppgifter. Olika roller som använder ett system kan ha olika behov av information och ska därför ha olika typer av behörigheter eller s.k. åtkomstprofiler. En förutsättning för rätt behörighetstilldelning är att informationen är strukturerad och klassad så att rätt åtkomstregler kan upprättas.

Inom vissa områden, som t.ex. vård och omsorg, behöver man ha (teknisk) behörighet till en stor mängd information. I akuta situationer måste kanske annan vårdande personal än den ordinarie ha åtkomst till patientinformation. Här behövs istället regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter.

Sådan åtkomstkontroll måste kompletteras med funktioner för uppföljning, övervakning och loggning. Detta kan – och ska – påverka användarna så att dessa avhåller sig från otillåtna men tekniskt möjliga operationer i ett system.

Systemägare bestämmer vilka som ska få tillgång till system som ingår i systemet och vilka behörigheter dessa ska ha. Verksamhetens art och dess krav på informationens konfidentialitet och riktighet, tillsammans med legala krav som lagar, föreskrifter och avtal, styr hur behörigheterna ska se ut.

För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

Varje användare ska ha ett unikt Användar-ID, dvs. gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas, se information under D.2.13).

Det ska finnas en process eller rutiner som underhåller och förvaltar behörigheter för ett system, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst.

Sådana processer eller rutiner måste vara kopplade till Söderhamn Nära så att tekniska förändringar genomförs. Systemägare IT ska säkerställa den del av rutinen som rör införande, förändring samt borttagning av åtkomst i IT-resurser. Exempelvis ska stark autentisering finnas för åtkomst till system som innehåller information med höga skyddskrav på konfidentialitet och riktighet.

Vid anställning, förändring av roll eller arbetsuppgifter samt vid upphörande av anställning ska rapportering göras omedelbart till Lön Hälsingland (HR) så att reglering sker i PersonecP.

Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

*Logghantering*
För att erhålla spårbarhet och att exempelvis möjliggöra incidentutredningar samt för att upptäcka avvikelser från legala eller interna regelverk bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med höga skyddskrav eller om regelstyrd behörighetshantering används istället för teknisk dito.

Då loggning används ska det finnas processer eller rutiner för dess hantering. Sådana ska innefatta hur loggning går till, hur loggar skyddas mot manipulation

och obehörig åtkomst, hur länge de sparas och hur de granskas. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av GDPR. Detta innebär bland annat att om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke.

Processer och rutiner för loggning ska följas upp och dokumenteras.

**Riktlinjer för behörighetshantering och loggning**

| | |
|---|---|
| C.3.1 | Det ska finnas dokumenterade processer och/eller rutiner för hantering av behörigheter och rättigheter till system. |
| C.3.2 | Varje användare ska ha ett unikt Användar-ID. |
| C.3.3 | Externa användares åtkomst bör vara tidsbegränsad samt föregås av sekretessavtal. |
| C.3.4 | Det ska finnas dokumenterade rutiner för logghantering i objekt. |
| C.3.5 | Höga skyddskrav på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk. |
| C.3.6 | Då regelstyrd behörighetshantering används istället för teknisk behörighetshantering är loggning av användares aktiviteter obligatorisk. |
| C.3.7 | Förändringar i anställningar och roller ska omedelbart rapporteras till personalavdelningen så att reglering sker i PersonecP. |
| C.3.8 | Uppföljning ska ske av behörighetshantering och logghantering i objekt. |

## C4. Ändringshantering

Ändringar i system ska ske i enlighet med Söderhamns kommuns beslutade system-förvaltningsmodell. Det innebär att ändringar ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen.

Ändringar kan bero på exempelvis, önskemål från verksamhet/användare, fel eller brister, förändringar i legala krav eller nya versioner från systemleverantörer.

Ändringar i system ska vara samordnade med Change management-processen inom Söderhamn Nära.

Avveckling av system ska ske på ett strukturerat sätt och i samråd med kommunarkivet så att information hanteras i enlighet med den kommungemensamma arkiveringsplanen.

Större förändringar i eller omkring ett system ska föregås av en riskanalys (se avsnitt C6 – Riskanalyser).

**Riktlinjer för ändringshantering**

| | |
|---|---|
| C.4.1 | Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system. |
| C.4.2 | Vid avveckling av system ska en plan upprättas för hur information ska migreras, raderas eller slutarkiveras (i enlighet med den kommungemensamma arkiveringsplanen). |

## C5. Användarinstruktioner

Systemägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett system. Användare ska utbildas enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering
- Behörigheter
- Särskilda instruktioner för hur konfidentiell information får hanteras, t.ex. känsliga eller skyddade personuppgifter
- Information om vad som loggas och konsekvenser av att bryta mot användarinstruktioner, t.ex. att ta del av eller sprida konfidentiell information
- Incidentrapportering – användare ska vara vaksamma på brister och incidenter i systemet och veta hur man ska rapportera dessa (se avsnitt C7 – Incidenthantering).
- Eventuell sekretessförbindelse - Användare är naturligtvis även skyldiga att följa riktlinjerna i Kapitel A.

**Riktlinjer för användarinstruktioner**

| | |
|---|---|
| C.5.1 | Informationssäkerhetsregler ska finnas med i användarinstruktioner. |
| C.5.2 | Det ska finnas särskilda instruktioner för hantering av konfidentiell information som t.ex. skyddade personuppgifter. |

## C6. Riskanalyser

Risker är tänkbara oönskade händelser som kan inträffa och som kan ha en negativ påverkan på mål. Antingen på mål med själva systemet eller på verksamheters mål. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens händelsen innebär.

Vid större förändringar, till exempel, större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst, ska en riskanalys genomföras där Söderhamns kommuns grundmetod för riskanalys ska användas. Det kan också vara förändringar utanför själva systemet eller dess kontroll som motiverar en riskanalys, exempelvis ägarbyte av en systemleverantör eller en omorganisation som berör den verksamhet som systemet stödjer.

Riskanalysens resultat ska dokumenteras. En riskanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och kan då tas med i kommande förvaltningsplan.

**Riktlinjer för riskanalyser**

| | |
|---|---|
| C.6.1 | Riskanalyser ska genomföras i samband med större förändringar i eller omkring system. |
| C.6.2 | Riskanalysresultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i förvaltningsplaner. |

## C7. Incidenthantering

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan, eller skulle kunnat, leda till brister i konfidentialitet, riktighet eller tillgänglighet i information. Systemägare ansvarar för att incidenter relaterade till system upptäcks, samlas in, hanteras, sammanställs och dokumenteras. Incidenter kan delas in i mindre incidenter och allvarliga incidenter (major incidents).

Mindre incidenter är t. ex. mindre tekniska fel i system eller att enstaka användare inte följer användarinstruktioner. I systemets användarinstruktioner ska det finnas rutiner för hur användare ska rapportera mindre incidenter (se C5 – Användarinstruktioner). Incidentrapporter ska mottas och lämpliga åtgärder ska vidtas.

Allvarliga incidenter är större störningar i ett system som t. ex. ett längre avbrott (några timmar eller mer), dataintrång eller infektion av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras enligt gällande mall för allvarliga IT-relaterade incidenter. Utredningen ska drivas av åtgärdsansvarig i samverkan med relevanta aktörer, och informationssäkerhetsansvarig.

Åtgärdsansvarig ska upprätta avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med Söderhamn Nära. (Se kapitel D)

En personuppgiftsincident ska rapporteras till Integritetsskyddsmyndigheten av berörd sektors åtgärdsansvarig med stöd av informationssäkerhetsansvarig, säkerhetskyddschef eller kommunjurist. Detta ska ske inom 72 timmar från incidentens uppdagande.

Flera fall av mindre incidenter av likadan art kan tillsammans utmynna i eller utgöra en allvarlig incident. Ett antal störningar i systemet av samma typ som var för sig betraktas som mindre incidenter kan tillsammans innebära en allvarlig incident.

Både mindre och allvarliga incidenter kan vara av akut art och behöva åtgärdas skyndsamt.

Sektorsamordnaren ska årligen sammanställa samtliga incidenter som är kopplade till verksamhetens olika system. Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i systemförvaltningsplaner.

För ytterligare information se Söderhamns kommuns anvisning informationssäkerhetsincident.

**Riktlinjer för incidenthantering**

| | |
|---|---|
| C.7.1 | Det ska finnas rutiner för hur användare ska rapportera incidenter. |
| C.7.2 | Akuta incidenter ska åtgärdas skyndsamt. |
| C.7.3 | Allvarliga incidenter ska utredas och dokumenteras enligt gällande mall. |
| C.7.4 | Avbrottsplaner ska upprättas som innehåller ansvarsförhållanden, kontaktpersoner och eskaleringsvägar. |
| C.7.5 | Samtliga incidenter som rör objektet ska dokumenteras och sammanställas. Kvarstående åtgärdsbehov ska tas om hand i förvaltningsplaner. |

### C8. Kontinuitetshantering

Krav på kontinuitet av driften av system sker i stora delar genom klassning. **Höga skyddskrav** för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

Avbrott kan dock ändå alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. Beroendet av funktionalitet i system kan ibland vara så högt att system helt enkelt inte får ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande även vid systemavbrott.

Nyckelpersonsberoende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersonal ska nyckelpersonberoendet åtgärdas t.ex. genom utbildning av ersättare. Nyckelpersonsberoende kan också minskas genom att använda vedertagen standard och standardprodukter.

**Riktlinjer för kontinuitetshantering**

| | |
|---|---|
| C.8.1 | Reservplaner och manuella rutiner ska finnas för kritiska objekt med höga skyddskrav gällande tillgänglighet. |
| C.8.2 | Nyckelpersonsberoende ska undvikas och åtgärdas. |

### C9. Kontroll av IT-tjänst

Verksamhetschef är ansvarig för informationssäkerheten inom sitt verksamhetsområde, det innebär även att säkerställa att dess processer, verktyg, personal och resurser har rätt skyddsnivå.

Korrekt informationssäkerhet ska säkerställas under hela livscykeln och innebär att verksamhetschef behöver försäkra sig om att rätt skyddsnivå är uppnådd och tydligt acceptera eventuella risker. Att avgöra rätt skyddsnivå innebär bland annat att genomföra verksamhets- och juridiska analyser genom informationsklassningar.

Förutom att kontrollera en IT-tjänst innan användning är det lämpligt att genomföra kontroller med jämna mellanrum i den frekvens som verksamheten finner lämpligt. Se även B.6.2 angående vägledning för kontroll av IT-tjänst.

**Riktlinjer för kontroll av IT-tjänst**

| | |
|---|---|
| C.9.1 | Innan en verksamhetschef börjar använda en IT-tjänst ska eventuella risker vara beaktade. |
| C.9.2 | Endast information som är klassad (informationsklassning) får användas i externa IT-tjänster och molntjänster. |
| C.9.3 | Gul - känslig information får endast lagras i en IT-tjänst som är tillräckligt kontrollerad, risken acceptabel och att lagringen av information inte bryter mot några författningar. |
| C.9.4 | IT-tjänster som lagrar konfidentiell information ska kontrolleras minst en gång om året. |

# Kapitel: D Informationssäkerhet i IT-miljön

IT-drift Säkerhetshandbok, Kommunens IT-driftsleverantör Söderhamn Nära

**Innehåll Kapitel D**



## D1. Övergripande ansvar för IT-avdelningen

- granska teknisk efterlevnad för att säkerställa att skyddsåtgärder införts korrekt
- genomföra olika säkerhets- och sårbarhetsgranskningar
- bedriva omvärldsbevakning för att underlätta identifiering och hantering av hot mot och sårbarheter i informationssystem
- stödja och följa upp övrig verksamhets arbete med informationssäkerhet
- sammanställa rapporter till ledningen

## D2. Ändringshantering

Förändringar i driftmiljö skall registreras i ärendehanteringssystemet där nedanstående punkter kontrolleras/dokumenteras:

- ansvarig beställare
- identifiering och registrering (genom registrering av ärende)
- konsekvensanalys (påverkade användare och system)
- information till verksamhet/systemägare
- information till IT-drift (normalt genom meddelande i Teams)
- plan för verifiering av funktion efter förändring, testprotokoll vid större förändringar
- plan för avbrytande av och återställande av misslyckade ändringar

- godkännande och driftsättning av förändring

Efter genomförda förändringar skall systemdokumentationen uppdateras. Ändringar som bedöms kunna påverka informationssäkerheten bör testas i separat testmiljö innan de införs i produktionsmiljön.

### D3. Uppdateringar och sårbarhetsskanning

I begreppet hantering av tekniska sårbarheter ingår att löpande underhålla befintliga installationer med säkerhetsuppdateringar samt att i lämplig omfattning kontrollera utvalda tjänsters säkerhetsnivå ex. genom sårbarhetsscanning/sårbarhetsanalys.

Central IT-infrastruktur i datacentret som servrar, databashanterare, brandväggar, nätverksutrustning skall bevakas efter sårbarheter genom omvärldsanalys. Det kan ske genom prenumerationer på utskick, deltagande i användargrupper, avtal med leverantörer, automatik i systemen eller liknande.

**Uppdateringar:**

- Uppdateringar som kan införas utan störningar bör ske med automatik
- Manuella uppdateringar ska normal införas månadsvis under servicefönster
- Akuta säkerhetsuppdateringar ska åtgärdas inom 3 dygn annars ska IT-chef och säkerhetschef meddelas.
- För system där uppdateringar inte kan avinstalleras eller systemen återställas från en systemkopia ska det finnas en plan för att backa tillbaka en uppdatering som orsakar störningar.
- För system som är isolerade ska det finnas en separat rutin för uppdateringar

**Sårbarhetsskaningar:**

- Ska ske minst halvårsvis
- Ska inkludera tjänster som är exponerade mot klientnätverk eller Internet
- Rapporter från säkerhetsskanningar sekretessklassas enligt OSL 18 kap. 13 §
- Kritiska sårbarheter som identifieras ska registreras i ärendesystemet på systemägaren alt. IT-chef. Åtgärd i form av uppdatering, omkonfigurering (workaround) eller isolering av systemet.

### D4. Härdning av system

Säkerhetskonfigurering eller härdning som det kallas i facklitteratur, innebär att komponenter, operativsystem, inbyggda programvaror, nätverkskomponenter, databaser och andra applikationer som ingår i ett informationssystem konfigureras på ett så säkert sätt som möjligt.

Exempelvis kan åtkomsträttigheterna i systemet och de delar som ingår begränsas, möjliga vägar till angrepp via sårbara funktioner i infrastrukturkomponenter och applikationer skäras av och exponering mot andra informationssystem eller externa enheter förhindras.

Skyddsåtgärder som ska övervägas vid uppsättning av system:

- Använda leverantörens säkerhetsrekommendation ex. Microsoft Security Baseline
- Begräsning av behörigheter (ex. ej lokal administratör)
- Inaktivering av onödiga tjänster
- Hårddiskkryptering
- Lokal brandvägg
- Skydd mot skadlig kod
- Vitlistning av programvara och hårdvara
- Plombering av anslutningar
- Detektering och skydd mot skadlig aktivitet
- Larm vid avvikande användning

### D5. Nätverksövervakning

Övervakningssystem för nätverksenheter såsom servrar, routrar och skrivare ska finnas för att åtgärda driftstörningar innan det blir ett problem för användarna. Systemadministratörer avgör vad som är lämplig nivå att övervaka med avseende på tillgänglighet och prestanda.

- Larm på kritiska fel skall skickas till driftspersonal och utanför normal arbetstid till beredskap.

### D6. Logghantering

- Loggar ska finnas för alla verksamhetskritiska system för att rekonstruera säkerhetshändelser.
- Loggar från verksamhetskritiska system ska granskas regelbundet manuellt eller genom automatisk larm vid avvikelser.
- Åtkomstloggar skall samlas till ett centralt loggsystem med utökad säkerhet.
- Åtkomstloggar sekretessklassas enligt OSL 18 kap. 8 §

### D7. Säkerhetsincidenter

En informationssäkerhetsincident påverkar eller kan komma att påverka driften negativt när det gäller konfidentialitet, tillgänglighet, spårbarhet och riktighet.

En informationssäkerhetsincident kan uppstå genom att:

- Obehöriga får tillgång till information (konfidentialitet)
- Verksamhetssystem inte är tillgängliga på avsett vis (tillgänglighet)
- Information är oriktig, förvanskad eller ofullständig (spårbarhet och riktighet)

Rapportering:

- Incidenter skall registreras i ärendehanteringssystemet med systemägare alternativt IT-chef som mottagare av information kring ärendet.
- Vid allvarliga informationssäkerhetsincidenter skall dataskyddsombud samt säkerhetschef meddelas.

För att avgöra vad som är en säkerhetsincident kan MSB:s exempel på vad som ska eller inte ska rapporteras användas som riktlinje

https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering/exempel-pa-it-incidenter-april-2016.pdf

## D8. Fysisk säkerhet

- Det är viktigt att fysiskt skydda den utrustning som hanterar informationen. Det fysiska skyddet ska förhindra obehörigt tillträde, skadegörelse och störningar i organisationens lokaler och informationsutrymmen.

**Tillträdesskydd**
Endast utsedd och behörig personal har tillgång till serverhallar och utrymmen med känslig information. Tillträdet registreras genom loggning i passagesystemet och dessa uppgifter hanteras i enlighet med gällande rutin.

I utrymmen med känslig information ska extern personal som till exempel servicepersonal, städpersonal med flera endast ges tillträde när det är nödvändigt. Besöksmottagaren ansvarar för att extern personal övervakas när behovet föreligger.

Dessa utrymmen ska vid behov även förses med kontroll för in- och utpassering. Tillträdet ska registreras och dessa uppgifter förvaras säkert. Ansvarig chef ansvarar för att utrymmena är säkrade.

**Brandskydd**
Datorer och annan elektronisk utrustning som lagringsmedia är känsliga för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns. Brandskyddet ska inaktiveras i serverhallen när arbete sker i lokalen för att förhindra att släckningsutrustningen utlöser av misstag.

**Vattenskydd**
Rör där vatten står under tryck bör inte finnas i säkra utrymmen. Vätskelarm ska finnas om det i utrymmet finns rördragningar innehållande vatten eller om det av andra orsaker finns risk för vattenskada.

**Klimatanläggning**
Temperaturen ska kunna mätas och regleras. Leverantörens rekommenderade underhållsplan för utrustningen ska i första hand följas.

**Elförsörjning**
Utrustning som kan behöva förses med avbrottsfri kraft (UPS) kan vara servrar, som exempelvis nätverksservrar, samt kommunikationsutrustning. Generellt är det tillräckligt om centrala servrar och datakommunikationsutrustningar skyddas mot ett elavbrott på cirka ett par timmar.

## D9. Krav på externa leverantörer

Vid upphandling av nya eller förändring av nuvarande system ska kontakt tas med IT-avdelningen för att stämma av att kraven stämmer överens med kommunens krav och IT-miljö. Det gäller oavsett om drift av systemet sker lokalt eller hos leverantör (molntjänst).

- Hanterar leverantören personuppgifter som personuppgiftsbiträde ska personuppgiftsbiträdesavtal upprättas med leverantören.
- Konsekvensbedömning och riskanalys ska genomföras vid extern drift.
- Hanteras sekretesshandlingar i leverantörens system ska det tecknas sekretessavtal om klausuler som reglerar sekretessen saknas i avtalet med leverantören.
- Sköter leverantören driften av systemet ska det tecknas ett IT-säkerhetsavtal om inte motsvarande krav ställts i upphandlingen eller regleras i annat avtal.

## D10. IT personals behörigheter

Avdelningschefen på IT ansvarar för behörighetshantering för personal inom IT-avdelningen. Behörigheter för personal inom IT-avdelningen och konsulter som börjar, slutar eller byter arbetsuppgifter ska hanteras. Detta omfattar godkännande, uppföljning och uppdatering av behörigheter.

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, som möjliggör för användaren att till exempel ändra rättigheter eller konfigurationer i applikationer, databaser, operativsystem eller nätverk ska begränsas till så få personer som möjligt

Systemadministrativa arbetsuppgifter ska vara kopplade till personliga användaridentiteter för att säkerställa spårbarhet avseende genomförda aktiviteter. För administratörer med omfattande behörigheter, där ovanstående inte kan tillämpas, ska särskilda skyddsåtgärder vidtas, till exempel upprättande av manuell åtkomstlogg.

## D11. Användarnas behörigheter

Systemägaren ska säkerställa att verksamhetssystemet är konstruerat så att alla rekommendationer avseende behörighetskontroll kan tillgodoses.

Systemägaren ansvarar för behörighetshantering i sitt eget system. Behörigheter för användare som börjar, slutar eller byter arbetsuppgifter ska hanteras när det gäller tilldelning, uppföljning och uppdatering av behörigheter.

Närmaste chef ansvarar för att användare före tilldelning av behörigheter ges tillräckliga kunskaper om gällande säkerhetsinstruktioner och instruktioner som speciellt ansluter till den egna arbetsuppgiften.

Minst en gång per år ska det kontrolleras att endast behöriga användare är registrerade i behörighetssystemet för verksamhetssystemet.

IT-driften ska kontrollera att beställningar i förändringar av rättigheter sker av behöriga beställare. Lista med behöriga beställare ska finnas på intranätet.

**Återställning av inloggningsuppgifter**
För den primära inloggningen ska det finnas tjänster för användarna att själva återställa sina inloggningsuppgifter.

Om IT-driften återställer inloggningsuppgifter för en användare ska det registreras i ärendesystemet och IT-driften ska säkerställa att det är rätt person som begär återställningen. Antingen användaren personligen eller en behörig beställare. Kontroll kan ske genom personkännedom, verifiering av uppringt telefonnummer eller motfrågor.

## D12. Anslutningar till externa leverantörer

Extern anslutning för extern leverantör till tjänster som tillhandahålls av Söderhamn Nära ska

- godkännas av systemägaren som tillsammans med IT-avdelningen ser över vilken autentiseringsmetod samt vilka tekniska lösningar som behövs.
- verifieras med minst två faktorer om det är tillfälliga anslutningar från okänd plats
- verifieras med certifikat eller motsvarande om det sker från en begränsad plats och från enheter som hanteras av leverantören
- ske med en krypterad anslutning
- vara möjligt att i efterhand följa upp i fråga om vem som kopplat upp sig, vid vilken tidpunkt och vilka resurser som utnyttjats
- konsultkonton inaktiveras när de inte är aktiva. Den som aktiverat kontot ansvarar för att Inaktivering sker.

**Systemägaren**

- beslutar och godkänner åtkomsträttigheter till endast information, program eller delar av operativsystemet som krävs för att kunna utföra uppdraget.
- uppdaterar systemsäkerhetsplanen enligt de beslut som har tagits avseende extern anslutning för extern leverantör.

## D13. Gruppkonton och servicekonton

**Gruppkonton**

- Låses till specifika datorer/tjänster
- Inga administratörsrättigheter

**Servicekonton**

- Lösenordslängd minst 20 tecken
- Blockeras från att logga in interaktivt
- Ej Domain Admin om möjligt, endast rättigheter som krävs för tjänsten

## D14. Mobil åtkomst och distansarbete

Systemägaren beslutar om ett verksamhetssystems information får bearbetas på distans med stationär och/eller mobil utrustning.

Regler (undantag får beslutas av systemägare eller säkerhetschef):

- Enheter som lagrar information för bearbetning i icke anslutet läge (offline läge) skall ha lokal lagring krypterad
- Anslutningar för mobil åtkomst eller distansarbete skall vara krypterade
- Anslutningar för mobil åtkomst eller distansarbete skall skyddas av minst två faktorer

## D15. Säkerhetskopiering och återställning

Gäller system i drift lokalt och omfattar ej molntjänster hos externa leverantörer.

**Uppdelning i tre olika klasser**

Det finns tre olika klasser med olika regler. Uppdelningen sker på servernivå vilket fungerar eftersom systemen i den virtuella miljön till stor del är separerade på olika servrar.

1. Specifika verksamhetssystem
Karaktär: lagrar i transaktionsdatabas, återställs sällan, hela systemet återställs, kritisk för att verksamheten ska fungera
Exempel: ProCapita, Raindance, Heroma

2. Gemensamma verksamhetssystem
Karaktär: lagrar enskilda objekt t.ex. filer eller epost, återställs relativt ofta, enskilda objekt återställs, viktig för att verksamheten ska fungera
Exempel: Filservrar, Exchange

3. Infrastruktur
Karaktär: Kritiska funktioner finns redundant, system kan vara nere utan att direkt störa verksamheten, återställs sällan, hela systemet återställs
Exempel: AD, DHCP, Print, IAS, WSUS

**Regler för de olika klasserna**

1. Specifika verksamhetssystem*

- Dygnskopior sparas i minst 1 vecka alternativt endast kontinuerligt skydd som sparas i minst 1 vecka.
- Veckokopior sparas i minst 4 veckor
- Inga månadskopior
- Kvartalskopior sparas i 2 år

2. Gemensamma verksamhetssystem*

- Dygnskopior sparas i minst 1 vecka
- Veckokopior sparas i minst 4 veckor
- Månadskopior sparas i minst 4 månader
- Kvartalskopior sparas i 2 år

3. Infrastruktur
- Dagliga säkerhetskopior sparas i minst 1 dygn
- Veckokopior sparas i minst 4 veckor
- Inga månadskopior
- Inga kvartalskopior

* För operativsystemet och programvara på servrarna till verksamhetssystemen gäller kraven för infrastruktur

**Tekniker för säkerhetskopiering, verifiering och återställning**
Det är tillåtet att kombinera flera olika tekniker för att uppfylla kraven på maximal dataförlust, lagringstid och återställning.
Exempel på tekniker för säkerhetskopiering: transaktionsloggar på flera ställen, skuggkopior (snapshots), replikering, traditionell programvara med tillägg för nästan omedelbar säkerhetskopiering.

Verifiering vid skrivning till hårddisk behövs ej, verifiering skall ske vid skrivning till band.

Återställning testas kvartalsvis enligt separat schema.

**Krav på lagringstekniker och förvaring**
- Säkerhetskopior får lagras på hårddisk, band eller annat lämpligt media.
- Minst en daglig säkerhetskopia skall förvaras i annan lokal än primärlagringen.
- Vecko- och månadskopior skall förvaras i annan lokal än primärlagringen.
- Alla kopior skall förvaras så att endast behörig personal har åtkomst.
- Förbrukad media/lagringsutrustning skall destrueras.

## Koppling till andra styrande dokument
Söderhamns kommuns informationssäkerhetspolicy

## Revideringshistorik och planerad revidering framåt
Styrdokumentet följs upp kontinuerligt. Dokumentet revideras vartannat år med start 2026.

---

KS § 349/231121
Dessa riktlinjer träder i kraft den 1 december 2023.