



# Riktlinjer för informationssäkerhet Kristianstads kommunkoncern

Ärendenummer	KS 2023/534
Dokumentansvarig	Kommunledningskontoret, Kommunstyrelsen
Beslutad av	
Datum och paragraf för beslut	2023-05-31
Ersätter tidigare beslut	2020-03-18 § 52
Giltig from	2023-05-31

# Innehåll

1.	Inledning .....	4
2.	Allmänt .....	4
3.	Mål .....	5
4.	Organisation .....	6
4.1	Avdelning för skydd och säkerhet .....	6
4.2	Digitaliserings & IT-avdelningen .....	6
5.	Hantering av informationstillgångar .....	6
5.1	Ansvar .....	6
	.....	8
5.1.2.	Roller inom informationssäkerhetsområdet .....	8
5.2	Offentlighet och sekretess .....	9
5.2.1.	Personuppgifter .....	10
5.2.2.	Personligt ansvar för hantering av all information .....	10
5.3	Klassificering .....	10
5.4	Handlingar .....	10
5.5	Säkerhetsskydd .....	11
6.	Personalsäkerhet .....	12
6.1.	Rekrytering .....	12
6.2.	Anvisningar informationssäkerhet .....	12
6.3.	Utbildning .....	12
7.	Användarsäkerhet .....	13
7.1.	Allmänna regler .....	13
7.2.	Privat användning .....	13
7.3.	Hem- och distansarbete .....	14
7.4.	Lokalt nätverk .....	14
7.5.	Externa nätverk .....	15
7.6.	Digital lagring .....	15
7.7.	Behörighet .....	16
7.8.	Lösenord .....	16
7.9.	Internet .....	17
7.10.	E-post .....	17
7.11.	Snabbmeddelande och kommunikationsverktyg .....	18
7.12.	Datavirus och skadlig kod .....	19
7.13.	Stöld och sabotage .....	19
7.14.	När anställningen upphör .....	19
8.	Systemanskaffning, systemförvaltning och avveckling .....	19
8.1.	Systemanskaffning .....	19
8.2.	Granskning och driftgodkännande .....	21
8.3.	Systemförvaltning .....	21
8.4.	Systemdrift .....	22
8.5.	Systemavveckling .....	22
9.	Kontinuitet och avbrott .....	22
9.1.	Kontinuitetsplanering .....	22
9.2.	Avbrott och återställning .....	23
10.	Incidenthantering .....	23

10.1.	Dokumentation av inträffade incidenter .....	23
10.2.	Rutiner för hantering och rapportering av säkerhetsincidenter .....	23
10.3.	Rutiner för hantering och rapportering av personuppgiftsincidenter .....	24
11.	Kontroll .....	24
11.1.	Kontroll av IT-användning .....	24
12.	Stöd och hjälp.....	25

## 1. Inledning

Information är en av Kristianstads kommunkoncerns viktigaste tillgångar. Informationen som behandlas i våra verksamheter har en stor roll i hur vi utför vårt arbete på ett effektivt sätt. Hoten mot vår information är därefter också väldigt stor. Det är således viktigt att vi arbetar strategiskt och effektivt för att skydda vår information.

Informationssäkerheten ska vara väl förankrad i verksamheten och den berör alla.

Dessa riktlinjer redovisar Kristianstads kommunkoncerns viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

- hur informationssäkerhetsarbetet ska bedrivas
- mål för informationssäkerhetsarbetet
- ansvar och roller inom informationssäkerhetsområdet
- generella regler och rutiner.

Riktlinjer för informationssäkerhet fastställs av kommunstyrelsen och respektive bolagsstyrelse.

Vissa anpassningar av delar av riktlinjerna kan förekomma inom de olika verksamheterna.

## 2. Allmänt

Utgångspunkter för informationssäkerhetsarbetet är:

- lagar, förordningar och föreskrifter
- ISO 27000
- avtal
- styrdokument.

Informationssäkerhetsarbetet ska säkerställa att kommunkoncernen kan tillhandahålla relevant information som uppfyller följande fyra aspekter:

- tillgänglighet – rätt information till rätt person vid rätt tillfälle
- riktighet – informationen skyddas så att obehörig inte kan ändra eller förvanska den
- konfidentialitet – informationen ska inte i strid med lagkrav eller kommunkoncernens riktlinjer göras tillgänglig eller delges obehörig
- spårbarhet – att i efterhand kunna spåra specifika händelser och aktiviteter till en användare eller objekt, för att kunna säkerställa vem som gjorde vad och när det skedde.

Informationssäkerhetsarbetet ska inriktas och bedrivas så att det blir en integrerad del av kommunkoncernens normala verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Riktlinjerna är bindande för alla delar av kommunens verksamhet och utgör en miniminivå för förvaltningarnas och bolagens verksamhet. Vissa verksamhetsspecifika anpassningar kan göras.

Det är inte tillåtet att använda kommunkoncernens informationstillgångar på ett sätt som strider mot riktlinjerna.

### 3. Mål

Målet med informationssäkerhet och riktlinjerna är att minska sannolikheten och konsekvensen för förlorad åtkomst till, informationsläckage eller förlust av information. Vidare måste kommunkoncernen även ha en tillräckligt hög ambitionsnivå för att uppfylla befintliga och kommande lagstiftningar inom informationssäkerhetsområdet.

Utgångspunkten för informationssäkerhetsarbetet i kommunkoncernen är att det ska vara riskbaserat, och ska så långt det är ekonomiskt och praktiskt möjlig tillämpa och följa standarden SS-ISO/IEC 27000.

Alla som arbetar inom kommunkoncernen, det vill säga förtroendevalda, medarbetare, praktikanter och externa utförare, ska ha kunskap och vara medveten om informationssäkerhetsfrågornas betydelse i kommunkoncernen.

Informationssäkerhetsarbetet ska bedrivas löpande så att

- all personal har kunskap om gällande informationssäkerhetsregler
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- gällande lagar, förordningar och föreskrifter följs
- ingångna avtal är kända och följs
- krishanteringsförmågan upprätthålls
- det finns tillgång till en säker och väl definierad infrastruktur för extern och intern datakommunikation
- alla investeringar både i form av information och teknisk utrustning skyddas i tillräcklig grad
- det framgår vilken klassningsnivå av information som ett system kan hantera på ett säkert sätt
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.

## 4. Organisation

### 4.1 Avdelning för skydd och säkerhet

Avdelningen för skydd och säkerhet på kommunens räddningstjänstförvaltning är den kommungemensamma resurs som stödjer den kommunala organisationen med sakkunskap kring de frågor som rör kommunkoncernens trygghets-, säkerhets- och krisberedskapsarbete.

Avdelningen svarar även för kommunövergripande stöd i och samordning av frågor som rör informations säkerhet, säkerhetsskydd samt krishantering och krisledning. Avdelningen leds av kommunens säkerhetschef som under kommundirektören ansvarar för intern och extern samordning av detta arbete.

### 4.2 Digitaliserings & IT-avdelningen

Digitaliserings & IT-avdelningen har i uppdrag att driva digitaliseringen och leverera verksamhetsstyrd IT. IT-avdelningen erbjuder behovsstyrda IT-tjänster och digitaliseringsstöd till verksamheterna. I en så kallad tjänstekatalog beskrivs de tjänster (standardtjänster och tilläggstjänster) som Digitaliserings & IT-avdelningen tillhandahåller.

Uppdraget innebär att förbättra den kommunala verksamheten genom att dra nytta av modern informations- och kommunikationsteknik samt dra nytta av nya kompetenser. Tjänsteutbudet ska vara verksamhetsdrivet och avdelningen verkar för god service. Digitaliserings & IT-avdelningen finns tillgänglig dygnet runt, alla dagar om året. Den övergripande målsättningen är att förbättra IT-stödet i kommunkoncernens verksamheter och att användare ska ha tillgång till de verktyg som de behöver i sitt arbete.

## 5. Hantering av informationstillgångar

### 5.1 Ansvar

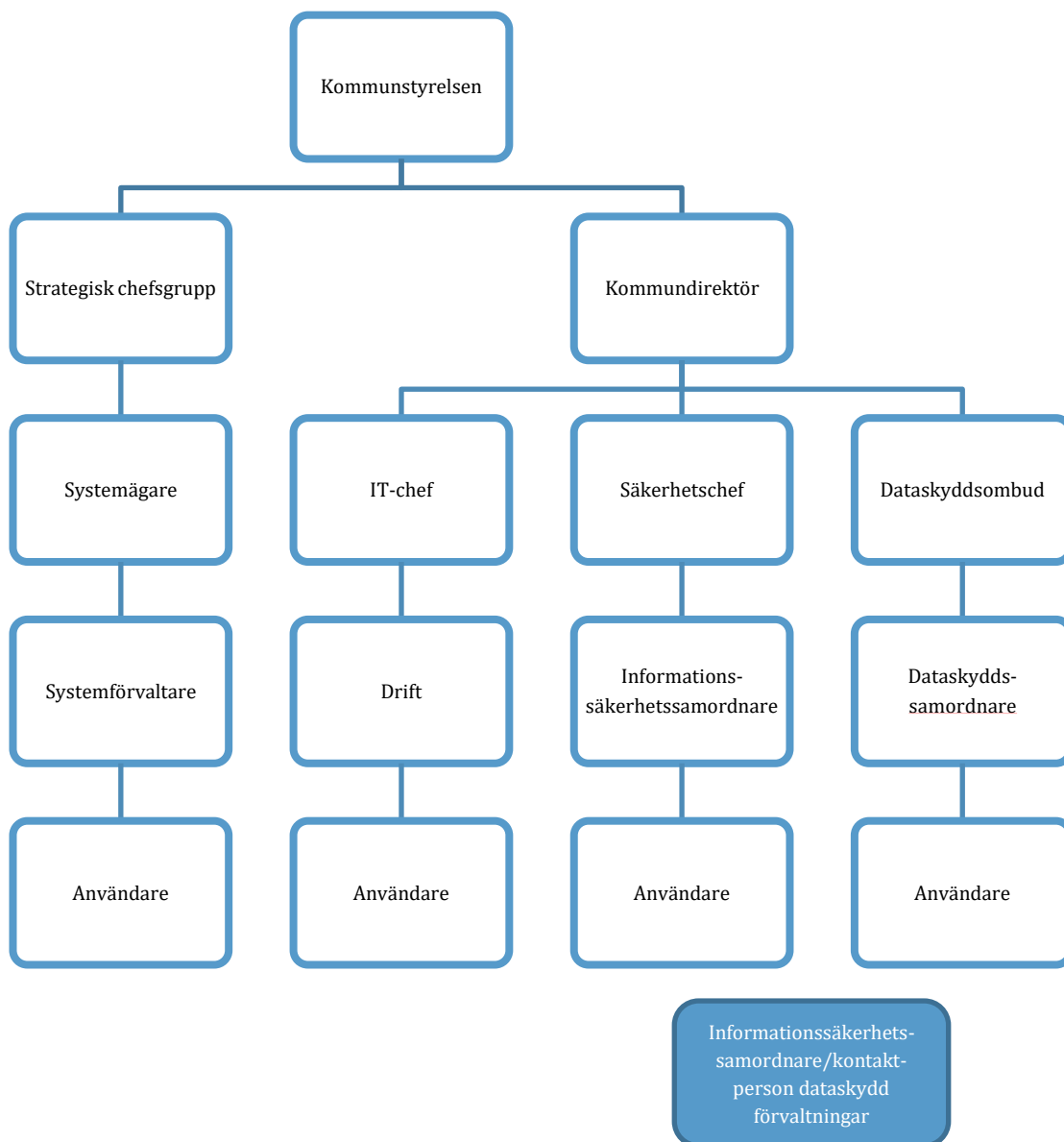
Ordinarie verksamhet ansvarar för informationssäkerhet och IT-säkerhet inom sitt verksamhetsområde. Detta styrs i kommunkoncernens säkerhetspolicy. När det gäller bolagen kan de ha egna policys som inte ska motsäga kommunkoncernens men som kan omfatta delar som är specifika för just bolagen. Detta innebär att inom respektive

ansvarsområde ansvarar chefer och medarbetare för att upprätthålla rätt nivå av informations säkerhet samt IT-säkerhet för de processer och resurser de ansvarar för. Varje nämnd och styrelse inom kommunkoncernen är personuppgiftsansvarig och har en utsedd kontaktperson för arbetet med verksamhetens dataskydd.

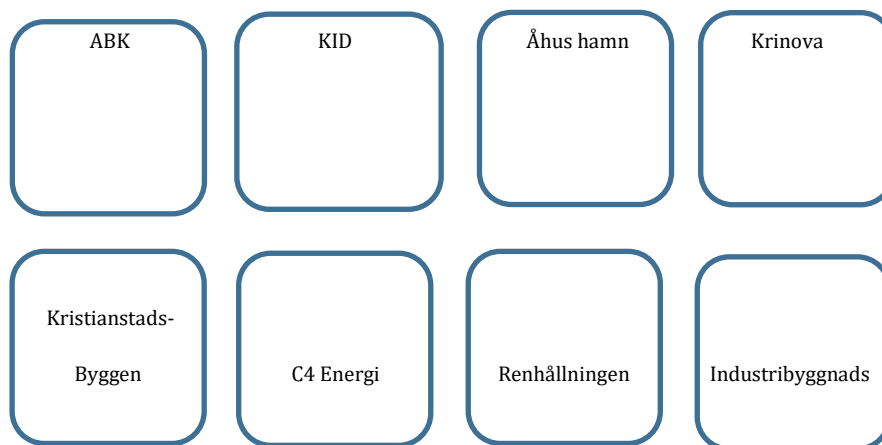
Stöd för det här arbetet ges från IT-avdelningen och informations säkerhetssamordnaren.

Ansvarsfördelningen ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla målen för informations säkerhetsarbetet.

Nedanstående bild och efterföljande text beskriver de olika roller och ansvar för informations säkerheten som finns inom kommunkoncernen.



## Bolagen



### 5.1.2. Roller inom informationssäkerhetsområdet

Respektive kommunal myndighet – det vill säga nämnd eller bolagsstyrelse – är informationsägaren för myndighetens information och ansvarar för den. De politiska nämnderna/bolagsstyrelserna är ytterst ansvarig för myndighetens information, men i praktiken är det oftast arkivansvarig som säkerställer att rollen uppfylls.

Enligt Arkivreglemente för Kristianstads kommun KF 2017-10-27 § 221 ska varje myndighet utse en arkivansvarig. Om inget annat anges är förvaltningschefen arkivansvarig.

Det övergripande ansvaret för kommunkoncernens Informationssäkerhet och IT-system vilar på kommunstyrelsen och respektive bolagsstyrelse.

Säkerhetschefen ansvarar för ledning av informationssäkerhetsarbetet och svarar under kommundirektören.

IT-chefen ansvarar för ledning av IT-säkerhet och svarar under kommundirektören.

På uppdrag av kommunstyrelsen ska strategisk chefsgrupp genom Digitaliseringsrådet svara för analys och beredning av IT-frågor.

Informationssäkerhetssamordnaren arbetar övergripande med samordning av informationssäkerhet i hela kommunen samt fungerar som en stödfunktion mot verksamheterna i frågor som rör informationssäkerhet.



Informationssäkerhetssamordnaren utses av kommunstyrelsen och svarar under säkerhetschefen.

På respektive förvaltning eller bolag kan informationssäkerhetssamordnare finnas som då ansvarar för arbetet med informationssäkerhet inom verksamheten.

Rollen som dataskyddssamordnare ansvarar för att samordna kommunens arbete rörande dataskydd.

Dataskyddsombudet agerar som kunskapsstöd inom kommunkoncernen samt med tillsyn och uppföljning av bland annat dataskyddsrelaterade risker.

Systemägare är respektive förvaltnings- eller bolagschef som på uppdrag från nämnd eller styrelse har ansvaret för att IT-systemet förvaltas på för verksamheten bästa sätt. Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-systemet inom ramen för resurstilldelningen för sin verksamhet.

Vid behov utser systemägaren en referensgrupp för sitt IT-system. Referensgruppen fungerar som en rådgivande funktion till systemägaren i frågor som rör systemförvaltningen och håller sig informerad om huruvida systemet stöder verksamheten.

Systemförvaltare utses av systemägaren och har ansvaret för den dagliga användningen av IT-systemet.

Användare av IT-systemet har att följa riktlinjer och instruktioner för informationssäkerheten samt att ta del av och följa de regler som finns för systemet.

IT-chefen är systemägare för kommunkoncernens tekniska IT-infrastruktur och ansvarar för att denna fungerar.

IT-driftansvarig utses av IT-chefen och ansvarar för att den dagliga driften upprätthålls enligt överenskommelse med systemägaren.

För IT-system som har gemensam leverantör eller är gemensamma för flera kommuner inom Skåne Nordost ska central systemägare, central systemförvaltare och central driftansvarig utses. Dessa ansvarar för samordningen med lokala systemägare, systemförvaltare och driftansvariga i respektive kommunkoncern.

## 5.2 Offentlighet och sekretess

Offentlighetsprincipen innebär att regeringens och myndigheters verksamhet så långt möjligt ska vara öppna för insyn och syftet är att garantera rättssäkerhet och effektivitet i förvaltningen och folkstyret. En följd av offentlighetsprincipen är att alla ska ha rätt att ta del av allmänna handlingar. Regler om allmänna handlingars offentlighet finns i Tryckfrihetsförordningen (TF) och hanteringen av dessa i Offentlighets- och sekretesslagen (2009:641) (OSL). Rätten att ta del av allmänna handlingar begränsas på många områden genom regler om sekretess som återfinns i huvudsak i OSL samt

författningar som OSL hänvisar till. Sekretess innebär förbud att röja en uppgift, vare sig det sker muntligen eller skriftligen, genom utlämnande av handling eller på annat sätt.

Handlingar kan vara allmänna eller icke allmänna. Handlingar som inte är allmänna är en myndighet inte skyldig att lämna ut. En handling anses allmän om den kan anses förvarad hos en myndighet samt att den är antingen inkommen dit eller upprättad där.

Alla allmänna handlingar måste samlas systematiskt så att handlingen kan återsökas. Ett minimikrav enligt OSL är att hemliga handlingar alltid måste registreras.

Om det är uppenbart att en allmän handling är av ringa betydelse för myndighetens verksamhet behöver den varken registreras eller hållas ordnad.

Den som begär ut en handling kan välja mellan att komma till myndigheten och på plats ta del av handlingen eller att få en kopia av handlingen. En begäran om att få ta del av allmänna handlingar ska behandlas skyndsamt. Vid en begäran om utlämnande måste en sekretessprövning företas av uppgifterna i den allmänna handlingen. Om handlingen inte bedöms omfattas av sekretess ska handlingen lämnas ut i sin helhet. Om handlingen bedöms omfattas av sekretess, helt eller delvis, ska sökanden erhålla ett överklagbart beslut om detta samt en hänvisning om hur överklagan ska göras.

### **5.2.1. Personuppgifter**

I dataskyddsförordningen (GDPR), 2016/679, regleras rätten att behandla personuppgifter. Syftet med förordningen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. På kommunens intranät finns information om behandling av personuppgifter.

### **5.2.2. Personligt ansvar för hantering av all information**

Oavsett om stödsystem används eller egna dokument skapas, har medarbetare och förtroendevalda ett personligt ansvar för säkerheten i sin hantering av information i alla dess former. I detta ansvar ingår bland annat att känna till de regler som gäller när information hanteras. När information hanteras, till exempel skrivs in, tas ut eller bearbetas, är den enskilde medarbetaren ansvarig för informationens riktighet och att den skyddas mot obehörig insyn.

## **5.3 Klassificering**

Den information som finns inom kommunkoncernen, oavsett form, är en tillgång för kommunkoncernen och måste därför också ha ett lämpligt skydd. Nämnderna ska klassificera informationen efter tillgänglighet, riktighet, konfidentialitet och spårbarhet före upphandling och vid anskaffning av system samt vid behov såsom större uppdateringar och lagändringar. Alla informationssystem ska sedan klassificeras med hjälp av SKR:s verktyg för klassificering, KLASSA eller motsvarande. Resultatet av en klassning i KLASSA bör underhållas av den som förvaltar och drifvar systemet.

## **5.4 Handlingar**

Klassificering (av handlingar och ärenden där klassificering sker) görs utifrån klassificeringsschema VerkSAM.

Klassificeringsschemat är inte någon fullständig klassificeringsstruktur för verksamhetsbaserad arkivredovisning, utan kan ses som en innehållsförteckning, som motsvarar de tre högsta nivåerna i verksamhetsbaserad arkivredovisning:

- Verksamhetsområde
- Processgrupp
- Process

Verksamhetsområden, processgrupper och processer som redovisas i klassificeringsstrukturen är hierarkiskt och systematiskt ordnade genom punktnotation. All klassificering sker på tredje nivån. Alla ärenden och handlingar får alltså en tresiffrig kod.

Klassificeringsstrukturen är verksamhetsbaserad och inte bunden till organisation. Strukturen utgår från vilken typ av verksamhet som handlingar/information uppkommer i, oberoende av hur verksamheterna är organiserade i kommunkoncernen.

Både ärenden och varje enskild handling ska klassificeras. Ett ärende kan alltså innehålla handlingar med olika klassificeringar.

Läs mer om detta på intranätet och i respektive förvaltnings dokumenthanteringsplan.

## 5.5 Säkerhetsskydd

Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada (men) som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser ska göras enligt följande prioriteringsskala:

1. kvalificerat hemlig vid en synnerligen allvarlig skada
2. hemlig vid en allvarlig skada
3. konfidentiell vid en inte obetydlig skada
4. begränsat hemlig vid endast ringa skada.

Det är upp till den som upprättar en handling att avgöra vilken säkerhetsskyddsklass som är aktuell.

Information som berörs av säkerhetsskydd får endast hanteras på fristående system utan nätverkssystem eller möjlighet till trådlös uppkoppling. Utrustning får därav inte hyras eller lånas in av extern part utan måste vara friköpt.

Datorer för detta ändamål ska vara tydligt märkta med information om att de innehåller säkerhetsskyddsklassificerade uppgifter, numrerade och registrerade på avdelningen för skydd och säkerhet. Handlingen i sig ska tydlig märkas med text i sidhuvud och sidfot om att den innehåller säkerhetsskyddsklassificerade uppgifter. Handskrivna handlingar ska i sig tydlig märkas med text i sidhuvud och sidfot om att den innehåller säkerhetsskyddsklassificerade uppgifter.

För utskrift av säkerhetsskyddsklassificerade uppgifter får endast fristående skrivare utan minne användas, ej nätverksanslutna skrivare. Skrivaren måste förvaras i ett säkerhetsskåp godkänt för säkerhetsskyddsklassificerade uppgifter, klassificerat enligt SS 3492.

Läs mer om säkerhetsskydd i Riktlinjer för säkerhetsskydd.

## 6. Personalsäkerhet

### 6.1. Rekrytering

Vid rekrytering ska informationssäkerhet beaktas. Den sökande ska kontrolleras på lämpligt sätt. Medför det åtkomst till sekretessbelagda uppgifter eller aktiviteter som omfattas ska kontroller bestämmas innan processen påbörjas. Kontrollerna som ska utföras måste stå i proportion till den berörda tjänsten.

Genom att underteckna anställningsbeviset godkänner och verifierar den nyanställde att man tagit del av och förbinder sig att följa dessa riktlinjer för informationssäkerhet samt ger ett medgivande för hantering av personadresserad post.

### 6.2. Anvisningar informationssäkerhet

Alla anställda ska vara väl medvetna om sitt ansvar för informationssäkerheten. I takt med nya och förändrade lagkrav har den anställda ett eget ansvar att sätta sig in i de berörda delarna. Informationssäkerhetssamordnaren ansvarar för att bedriva omvärldsbevakning och följa upp att nya och förändrade lagkrav efterföljs samt samordnar vid behov utbildning på området inom kommunkoncernen.

### 6.3. Utbildning

Kompetens och medvetenhet är en viktig del i arbetet med informationssäkerhet, framför allt ger den en trygghet för både den anställde och verksamheten.

Alla anställda ska genomföra DISA, eller motsvarande, en grundläggande utbildning inom informationssäkerhet som MSB, Myndigheten för samhällsskydd och beredskap, tagit fram. Utbildningen görs lämpligast vid anställningens början för att öka medvetenheten hos den anställde. Varje verksamhets enhetschef har som ansvar att se till att deras anställda har genomfört utbildningen.

Vid större förändringar, exempelvis lagändringar, som påverkar vårt arbete i kommunen gällande informationssäkerhet och IT ska det tas fram separata utbildningar inom detta område för att öka kunskapen och medvetenheten om förändringen.

Systemägaren och/eller verksamhetens chef ansvarar för att användarna och i förekommande fall även leverantörer erhåller lämplig utbildning och fortbildning för att öka medvetenheten.

Den anställde har ett eget ansvar att se till att denne har den kunskap som efterfrågas inom informationssäkerhet. Känner den anställde att den saknar kunskap är det den anställdes ansvar att påtala detta för sin chef så att utbildning kan ges inom det område som den anställde brister i.

## 7. Användarsäkerhet

### 7.1. Allmänna regler

För att uppnå nödvändig IT-säkerhet gäller följande regler för användning av IT-systemen:

- all installation och konfiguration av digital utrustning ska ske av behörig tekniker
- kommunala inloggningsuppgifter får inte sparas i privat utrustning
- endast godkända program får installeras och användas på digital utrustning eller nätverk
- när det gäller applikationer (appar) som laddas ned till mobiltelefoner och annan digital utrustning tillåts vissa applikationer inte av säkerhetsskäl inom Kristianstads kommun. Beslut om vilka applikationer som ej tillåts tas av avdelningen för skydd och säkerhet.
- det är inte tillåtet att kopiera eller använda programmen utanför kommunkoncernens verksamhet
- vid fel på digital utrustning ska detta omgående anmälas till IT-Servicedesk eller motsvarande som gäller för den verksamheten
- skydda digital utrustning mot stöld eller intrång. Fråga okända personer om deras ärende. Placera om möjligt utrustningen så att den inte syns utifrån
- vid kortare frånvaro lås för inloggning. Vid längre frånvaro ska utloggning göras. Vid arbetsdagens slut ska utrustningen stängas av
- var aktsam med digital utrustning.
- Sefos finns för att kunna skicka säkra meddelanden eller genomföra säkra videomöten som behandlar eller innehåller information som omfattas av sekretess, känsliga eller integritetskänsliga uppgifter dvs motsvarande klassningsnivå 3 till 4 enligt informationsklassningsmatrisen. Läs mer i Tillämpningsriktlinjen för Sefos på intranätet.
- Säker scanning kan användas om ni har information som inte får hanteras i molnet. All kommunikation går direkt mellan lokal skrivare och en server/lagringssyta som står i kommunens serverhall.

### 7.2. Privat användning

Den digitala utrustningen får användas för privat bruk och då endast på ett sådant sätt att arbetet och den digitala utrustningens funktion inte blir lidande eller skadar kommunkoncernens anseende och förtroende. Det är inte tillåtet att titta eller lyssna på material med pornografiskt eller rasistiskt innehåll. Förbudet gäller även annat material som är diskriminerande eller har anknytning till kriminell verksamhet. Surf och användande av sociala medier för privata ändamål, får endast göras till pålitliga källor och om arbetet inte blir lidande. Användning av e-post för privata ändamål är tillåten vid

enstaka tillfällen, i begränsad omfattning och om arbetet inte blir lidande. Det är aldrig tillåtet att använda kommunkoncernens e-postadress för registrering på privata forum.

När det gäller användning av mobiltelefoner kan det vara svårt att dra en gräns mellan arbetstid och fritid. Medarbetare kan använda mobil enhet för privat användning för samtal och datatrafik inom Sverige i begränsad omfattning och så att verksamheten inte blir lidande. Våra abonnemang fungerar att använda utomlands utan att IT behöver göra något.

Det är användarens ansvar att kolla vad det kostar att använda mobilen i det land man ska till.

Utlandssamtal kan ge löneavdrag om de inte är arbetsrelaterade, stäm alltid av med din närmaste chef innan du reser utomlands om du ser ett behov av att använda din arbetsmobil.

Det är operatörens priser som gäller för samtal från din arbetsmobil till abonnent i utlandet.

Alla abonnemang från 044 -13 nummer är stängda för utlandssamtal och betaltjänster. Mobilabonnemang är spärrade för betaltjänster men inte för utlandssamtal. Om medarbetarens anställning kräver möjlighet till utlandssamtal kan detta beställas hos IT-avdelningen. Beställning kan även göras för begränsad tid.

### 7.3. Hem- och distansarbete

Om privat digital utrustning används för hem- eller distansarbete kan denna vara en säkerhetsrisk. Tänk på att:

- inte kopiera känslig information till digitalt media som sedan tas med utanför ordinarie arbetsplats
- inte lagra sekretessbelagd eller för verksamheten känslig information på privat digital utrustning
- information som används i extern miljö och lagras på externa lagringsmedia inte får användas i kommunkoncernens nätverk utan att viruskontroll har skett.
- det är av stor vikt att om digital utrustning delas med flera i hemmet ska utloggning göras vid frånvaro

För distansarbete, tillfälligt arbete utanför ordinarie arbetsplats och vid arbete under resa till och från arbetsplatsen finns särskilda riktlinjer.

### 7.4. Lokalt nätverk

Nätverket är en viktig gemensam resurs som ger alla möjlighet att lagra information, dela på skrivare och program, upprätta kommunikation med mera. Vid användning av nätverket gäller följande:

- inloggning på nätverket ska ske med personligt konto och lösenord, all annan inloggning är förbjuden
- det är tillåtet att använda streamingtjänster såsom webbradio, musik- och

- filmtjänster om detta behövs i arbetet
- det är förbjudet att skaffa sig rättigheter utöver de som tilldelats.

Alla aktiviteter i nätverket loggas. Loggningsfunktioner används för att spåra obehörig verksamhet och intrång. Detta görs för att skydda informationen samt för att undvika att oskyldiga misstänks om oegentligheter inträffar.

## 7.5. Externa nätverk

Att använda den digitala utrustningen i andra nätverk än kommunkoncernens lokala nätverk kan innebära en säkerhetsrisk då information exponeras för obehöriga. Tänk på att:

- vara uppmärksam vid anslutning till andra nätverk
- att inte upplåta/dela digital utrustning för extern anslutning.

## 7.6. Digital lagring

Var allmänna handlingar ska lagras framgår i varje myndighets dokumenthanteringsplan.

I myndighetens dokumenthanteringsplan finns bestämmelser om var kommunens allmänna handlingar ska förvaras, hur länge en allmän handling ska sparas, och andra hanteringsanvisningar. Kristianstads kommuns dokumenthanteringsplaner finns på kommunens intranät och externa hemsida.

Informationen i våra verksamheter ska hanteras, struktureras och gallras på ett sätt som uppfyller de bestämmelser som finns i bland annat tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen samt de bestämmelser som finns i kommunens riktlinjer och övriga styrdokument. Bestämmelser om informationshantering i kommunen finns bland annat i:

- Arkivreglementet
- Riktlinjer för bevarande av digitala allmänna handlingar
- Handbok för dokument- och ärendehantering

Varje förtroendevald, chef och medarbetare ansvarar för att de hanterar sin information i enlighet med befintliga riktlinjer.

Gallringsbeslut för till exempel skräppost, egna minnesanteckningar som inte tillför något till ett ärende och rutinartade frågor finns i [Kommunövergripande gallringsplan för handlingar av liten och kortvarig betydelse](#).

Tillämpningsriktlinjer för lagring i samband med användandet av molntjänster återfinns på intranätet.

Om information lagras lokalt på till exempel hårddisk, USB-minne eller liknande kan informationen förloras vid t ex en diskkrasch. Dessutom förhindras kollegor att vid behov komma åt informationen. Detta lagringsalternativ rekommenderas således inte.

Inget privat material i form av exempelvis text, musik, film, bilder, program får sparas på lagringsenheter i nätverket eller på lokala hårddiskar. Motiven för detta förbud är ökade säkerhetsrisker och risk för virusangrepp. Dessutom ökar kostnader för lagring och säkerhetskopiering.

Den information som hanteras i våra verksamheter ska hanteras, struktureras och gallras på ett sätt som uppfyller de bestämmelser som finns i bland annat tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen samt de bestämmelser som finns i kommunens riktlinjer och övriga styrdokument. Bestämmelser om informationshantering i kommunen finns bland annat i:

- Arkivreglementet
- Riktlinjer för bevarande av digitala allmänna handlingar
- Handbok för dokument- och ärendehantering

Varje förtroendevald, chef och medarbetare ansvarar för att de hanterar sin information i enlighet med befintliga riktlinjer, enligt ärende och dokumenthanteringspolicyn för Kristianstads kommun.

Var allmänna handlingar ska lagras framgår i varje myndighets dokumenthanteringsplan.

## 7.7. Behörighet

Kommunkoncernens IT-system, som nätverk, servrar och program, är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt informationen. De behörigheter som tilldelas i våra IT-system beror på arbetsuppgifter och avgörs av närmaste chef. I samband med att behörighet erhålls krävs att medarbetare och förtroendevalda har informerats om denna användarinstruktion och har genomgått utbildning i de IT-system som är aktuella att använda. När medarbetare eller förtroendevald har blivit upplagd som användare får hen en användaridentitet (konto) och ett lösenord.

Det är också viktigt när användare slutar att behörigheter tas bort/inaktiveras oavsett vilket system det gäller.

## 7.8. Lösenord

Vid en anställnings påbörjan tilldelas användaren ett datorkonto med tillhörande lösenord. Detta lösenord kan endast användas vid en första inloggning. När första inloggning görs kommer ett tvingande byte av lösenord. Även för övriga system som behörighet tilldelats måste det initiala lösenordet bytas mot ett eget. Lösenordet är personligt och hanteras därefter.



Därför ska:

- lösenordet skyddas väl
- lösenord inte avslöjas för andra eller lånas ut
- lösenord omedelbart bytas vid misstanke om att någon känner till det
- lösenord bytas med fastställda intervall.

Lösenordet ska bestå av minst åtta tecken och konstrueras så att det inte lätt kan kopplas till enskild person. Återanvänd inte tidigare använda lösenord. Om lösenordet glöms bort och inloggningsförsök görs med ett felaktigt sådant, kommer datorkontot att låsas efter ett visst antal försök. Om detta inträffar, kan användaren själv antingen nyttja de återställningstjänster som finns eller kontakta IT-ServiceDesk (för lösenord till datorkonton) eller systemförvaltaren (för lösenord till IT-system).

Det finns ett system för självservice avseende lösenordshantering till datorkonton. Det innebär att medarbetare och förtroendevalda själv kan återställa och/eller byta till ett nytt lösenord om det gamla glömts bort.

Om inloggning sker med e-legitimation, exempelvis BankID eller SITHS kort, behövs ingen hantering av lösenord. Det är viktigt att kortet förvaras på ett säkert sätt och att kortets PIN-kod inte avslöjas.

Lösenordsfiske är inom IT-säkerhet metoder för att manipulera personer till att utföra handlingar eller avslöja konfidentiell information. Lämna aldrig ut kontoinformation till okända mottagare.

## 7.9. Internet

Kommunkoncernens lokala nätverk är anslutet till Internet. All in- och utgående trafik sparas i en loggfil som visar vilka webbplatser som besökts. All nedladdning ska vara arbetsrelaterad och komma från pålitlig källa. Förutom säkerhetsrisken kan en felaktig hantering innebära skadeståndskrav t ex vid brott mot upphovsrätten. Det är inte tillåtet att via internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också annat material som är diskriminerande eller har anknytning till kriminell verksamhet. Det är inte heller tillåtet att använda arbetsredskap för spel annat än i verksamhetssyfte. I specifika fall kan det dock vara motiverat för arbetet att besöka sidor som normalt är förbjudna, t ex vid utredningar, omvärldsanalyser, pedagogisk verksamhet. Informera och rådgör med närmaste chef vid tveksamhet.

Vid surfing på internet och användande av sociala medier så representerar medarbetare och förtroendevalda kommunkoncernen och man skall därför använda ett vårdat språk.

## 7.10. E-post

E-post är ett arbetsverktyg via molntjänst, och därför ska informationsklassning beaktas för vad som kan skickas via e-post, samt att gallring ska göras regelbundet. Eftersom kommunen är en bred organisation skiljer sig därmed både informations-behandling och informationstyper åt mellan våra olika verksamheter. Informationsklassning och

bedömningar utifrån dessa enskilda behov är ett ansvar som åligger respektive verksamhet.

Tillämpningsriktlinjer för användande av e-post i molntjänster återfinns på intranätet.

E-post med bilagor eller länkar kan utgöra ett hot när det gäller spridning av virus. Var uppmärksam på falska e-postmeddelanden. Vid misstanke om oegentligheter öppnas inte bilaga eller länk och kontakt tas med IT-ServiceDesk (eller motsvarande).

Inkommande e-post ska, liksom vanlig post och fax hanteras så snart som möjligt, normalt samma dag som handling inkommer till kommunkoncernen. Vid frånvaro ska annan användare hantera inkommen e-post på samma sätt.

För hantering av e-post gäller dessutom att:

- samma regler för vanliga brev
- känsliga personuppgifter och sekretessbelagt material ska inte skickas eller vidarebefordras i Outlook, för detta ändamål ska Sefos användas. Det ligger på varje förvaltnings och bolags ansvar att avgöra baserat på typ av uppgifter och mottagare, se respektive verksamhets informationsklassning och dokumenthanteringsplan
- personnummer är särskilt skyddsvärda personuppgifter och kräver ett högt säkerhetsskydd. Huvudregeln är därför att personnummer inte ska skickas via e-post. Emellertid kan personnummer skickas internt via e-post genom Outlook förutsatt att vi behöver uppgiften för att kunna driva verksamheten och det inte finns ngt annat rimligt alternativ. Observera att detta inte gäller för t.ex. personnummer som omfattas av socialtjänstens sekretess. Dessa ska inte hanteras i vanlig e-post. Andra kommunikationsvägar ska användas vid dessa tillfällen, t.ex. SEFOS.
- användning för privata ändamål är tillåten vid enstaka tillfällen, i begränsad omfattning och om arbetet inte blir lidande
- fylla i ärendefältet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i meddelandefältet, men inte skriva känslig information i ärendefältet
- alltid avsluta med personlig signatur i enlighet med kommunkoncernens grafiska handbok (eller motsvarande)
- det inte är tillåtet att vidarebefordra e-post automatiskt till mottagare utanför kommunkoncernen
- vara selektiv med att skicka till många mottagare samtidigt och med att skicka eller vidarebefordra meddelanden som innehåller stora filer
- kontakta närmaste chef om hotelsebrev eller liknande kommer och radera inte e-postmeddelandet.
  
- e-posten ska regelbundet rensas och gallras

### 7.11. Snabbmeddelande och kommunikationsverktyg

Teams eller liknande kommunikationsverktyg är tänkta som komplement till e-post i det dagliga arbetet och används i huvudsak till korta och snabba meddelande kollegor emellan. Dessa meddelanden sparas automatiskt.

Det är möjligt att använda dessa verktyg vid kommunikation även utanför kommunkoncernens nät. Informationsklassning ska beaktas för vad som kan skickas via dessa kommunikationsverktyg, samt att gallring ska göras regelbundet. Eftersom kommunen är en bred organisation skiljer sig därmed både informationsbehandling och informationstyper åt mellan våra olika verksamheter. Informationsklassning och bedömningar utifrån dessa enskilda behov är ett ansvar som åligger respektive verksamhet.

### **7.12. Datavirus och skadlig kod**

Datavirus kan beskrivas som ett program eller en programsekvens vars uppgift är att kopiera sig själv och tränga in i andra program för att utföra något otillbörligt. Kommunkoncernen har programvaror för viruskontroll och det görs kontinuerligt kontroll i nätverket. Även filer på externa lagringsenheter och filer som hämtas från Internet kontrolleras av antivirusprogram i nätverket. Eftersom det hela tiden tillverkas nya datavirus är det ändå viktigt att vara uppmärksam på problemet.

Vid misstanke om att systemet innehåller virus ska nätverkskabeln dras ut alternativt trådlös anslutning kopplas ifrån. Om e-post med virusvarning kommer, ska inte meddelandet skickas vidare. I samtliga dessa fall, anmäl omedelbart per telefon till IT-Servicedesk.

### **7.13. Stöld och sabotage**

Vid misstanke om stöld, sabotage, intrång etc. ska närmaste chef och IT-Servicedesk (eller motsvarande) kontaktas.

### **7.14 När anställningen upphör**

När medarbetare och förtroendevalda ska sluta sin anställning eller sitt uppdrag ska närmaste chef/politisk organisation avgöra hur arbetsmaterial ska hanteras i samråd med berörd och hur den digitala utrustningen återlämnas. När anställningen upphör avslutas datorkontot.

Det är av vikt att behörigheter till verksamhetssystemen avslutas. Chef är ansvarig att skicka in anmälan om avslut av behörigheter.

## **8. Systemanskaffning, systemförvaltning och avveckling**

### **8.1. Systemanskaffning**

När behov uppstår av större förändringar av befintligt IT-stöd eller av ett helt nytt IT-stöd ska samråd ske inom hela kommunkoncernen, där så är relevant.

I de fall samverkan kan ske utses en projektledare och en projektgrupp bestående av verksamhetsföreträdare, en tekniskt ansvarig och en upphandlingsansvarig. Vid behov utses även en styrgrupp, till vilken projektledaren rapporterar.

Om samverkan med en eller flera andra parter inte är möjlig, ansvarar den verksamhetsansvarige chefen för systemanskaffningsprojektet.

Projektledaren eller verksamhetsansvarig chef utformar en projektplan för nyanskaffningen. Denna ska omfatta:

- en beskrivning av verksamhetens behov
- mål med nyanskaffningen
- en tidplan
- resursbehov (personella och ekonomiska)
- en plan för när och hur uppföljning, utvärdering och avrapportering ska ske
- en plan för när och hur medarbetarna ska informeras och utbildas.

Projektledaren och verksamhetsansvarig chef sammanställer också en kravspecifikation. Denna ska innehålla:

- en risk- och sårbarhetsbedömning som klarlägger
  - verksamhetens krav på säkerhet avseende sekretess, riktighet och tillgänglighet
  - tilläggskrav i form av rättsliga, verksamhets- och hotrelaterade krav
  - krav på och beroende av kommunikation (internt och externt)
  - reservrutiner
  - krav på integration med andra system, samt
  - en konsekvensbedömning om personuppgifter behandlas på ett sätt som sannolikt leder till hög risk för de registrerades fri- och rättigheter.

Ansvarig för nyanskaffningsprojekt förbereder överlämnandet från test och utveckling till drift och förvaltning tillsammans med tilltänkt systemägare, systemförvaltare och IT driftsansvarig. Beslut om tidpunkt från vilken systemet övergår från projekt till förvaltning fattas av systemägaren. I och med detta övergår det operativa ansvaret till systemförvaltaren som då också övertar all dokumentation.

Projektplan och kravspecifikation överlämnas till styrgruppen för godkännande.

Nyanskaffning kan ske genom avrop från tillämpligt ramavtal eller genom upphandling i enlighet med lagen om offentlig upphandling. Om möjligt ska standardprodukter användas.

Vid införande av nya IT-system ska nämnder - och bolag som beslutat följa kommunens beslut om arkiv- och informationshantering - följa Riktlinjer för bevarande av digitala allmänna handlingar. Myndigheten ska säkerställa att informationen som lagras i IT-system bland annat kan struktureras, gallras och exporteras. Därtill ska myndigheten tillgodose kravet om systemdokumentation för systemet. Därför är det viktigt att myndigheten ställer tydliga arkivkrav vid systemupphandling. Vid behov ska kommunarkivet rådfrågas vid upphandling av nya IT-system.

## 8.2. Granskning och driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett IT-system uppfyller ställda säkerhetskrav.

I samband med att en systemförvaltningsplan upprättas ska IT-systemet säkerhetsgranskas och klassificeras av verksamheten (systemägare och systemförvaltare) och uppfylla:

- relevant säkerhetsnivå
- de tilläggskrav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav.

Driftgodkännandeprocessen relateras till aktuell systemförvaltningsplan och ska omfatta:

- avgränsningar
- granskning av säkerhetsåtgärder i IT-systemet
- utvärdering av granskningen i förhållande till systemförvaltningsplanens krav
- redovisning av beslutsunderlag
- förslag till beslut.

Beslutsförslaget kan vara en rekommendation att:

- driftgodkänna IT-systemet
- driftgodkänna IT-systemet efter beslut om kompletterande säkerhetsåtgärder och när dessa ska vara genomförda
- inte driftgodkänna IT-systemet.

Systemägaren beslutar om driftgodkännande. Beslutet baseras på genomförd granskning i klassningsverktyget och säkerhetsutvärdering, som i sin tur bygger på en jämförelse mellan verksamhetens krav och vidtagna säkerhetsåtgärder.

PUB-avtal ska också tecknas i samband med upphandling av nytt system.

## 8.3. Systemförvaltning

Med systemförvaltning avses samtliga aktiviteter som görs för att styra, administrera och utveckla existerande system och stödja användandet (rätta, uppdatera, ändra, komplettera, utveckla med mera).

Vid samverkan kring förvaltning och drift av ett IT-system utses en central systemägare, en central systemförvaltare och en central driftansvarig.

För samhällsviktiga och gemensamma system ska en systemförvaltningsplan upprättas. Av denna ska framgå:

- om systemet omfattas av tilläggskrav i form av rättsliga krav, specifika verksamhetskrav och hotrelaterade krav
- systemägarens krav på kontinuitetsplan.

Om de förutsättningar som legat till grund för systemförvaltningsplanen förändras ska planen revideras. IT-avdelningen ansvarar för att ta fram och underhålla mallen för systemförvaltningsplanerna.

## 8.4. Systemdrift

Regler för systemdrift ska omfatta bland annat:

- systemdokumentationer
- driftdokumentationer
- bemanningsplan
- tillträdes- och brandskydd
- elförsörjning
- regler för säkerhetskopiering
- regler för förvaring av datamedia.

Kommunkoncernens interna nätverk ska vara dokumenterat i en särskild systemförvaltningsplan.

## 8.5. Systemavveckling

Innan ett IT-system som hanterar allmänna handlingar avvecklas måste informationsägaren/ägarna säkerställa att bestämmelser i lagar och styrdokument uppfylls. Bestämmelser gällande hantering av allmänna handlingar finns exempelvis i arkivlagen, varje myndighets dokumenthanteringsplan och kommunens arkivreglemente.

Systemägaren beslutar om när ett IT-system ska avvecklas. Vid avveckling ska särskilt uppmärksammas:

- Arkivlagen och myndighetens dokumenthanteringsplan
- vad som ska tas ut ur systemet före avveckling (på papper eller datamedia, e-arkivering)
- om systemet innehåller ärenden vilka behöver avslutas
- om återläsning av innehållet måste kunna ske längre fram
- om uppgifter behöver flyttas över till ett annat IT-system.

# 9. Kontinuitet och avbrott

## 9.1. Kontinuitetsplanering

Det ska i händelse av kris eller katastrof finnas en kontinuitetsplan för varje verksamhet inom kommunkoncernen. En kontinuitetsplan ska innehålla återstartsplaner och annan information som behövs om en allvarlig störning eller katastrof skulle inträffa.

Grunden till kontinuitetsplanen utgörs av en riskanalys av informationssystemens sårbarheter samt vilka hot som kan finnas mot verksamheten.

Hot kan till exempel vara:

- brand och elavbrott
- översvämning och explosion
- förlorad kommunikation
- naturkatastrofer
- hackers, trojaner och virus
- terrorister, vandalisering eller sabotage
- förlorade data eller behörighet
- felaktigt införda system
- bristande rutiner och otydliga roller och ansvar.

I kontinuitetsplanen ska det finnas identifierat vilka system som för verksamheten är mest kritiska och i vilken ordning dessa ska återstartas.

En kontinuitetsplan kan till exempel innehålla:

- scenarier
- organisation och ledning
- återstartsrutiner och plan för återstart av system
- rutiner för reservdrift och inkoppling av reservkraft
- alternativt driftställe
- inventarielista och licenser
- kontaktuppgifter
- manuella reservrutiner
- hur man ska gå tillväga för att aktivera planen
- testplan
- krisarbetsplats för åtkomst till datorhall.

Kontinuitetsplanen ska testas regelbundet och uppdateras vid förändringar.

## 9.2. Avbrott och återställning

Vid ett driftavbrott ska orsaken till avbrottet undersökas så snabbt som möjligt med de resurser som finns tillgängliga och med hjälp av dokumentation samt information från eventuella tidigare inträffade och liknande avbrott. Berörda system ska återställas snarast möjligt och med så liten informationsförlust som möjligt.

# 10. Incidenthantering

## 10.1. Dokumentation av inträffade incidenter

Incidenter ska i samtliga fall dokumenteras i syfte att snabbt kunna åtgärda liknande incidenter om de skulle inträffa igen.

## 10.2. Rutiner för hantering och rapportering av säkerhetsincidenter

När en incident sker ska detta rapporteras och hanteras utan dröjsmål. Detta för att minimera skada, åtgärda brister och utreda eventuell brottslighet.

När en anmälan kommit in om att en eventuell säkerhetsincident har inträffat eller om en incident på annat sätt har upptäckts ska loggar analyseras i syfte att säkerställa vilka användarkonton som varit aktuella alternativt om det är ett externt angrepp. Därefter ska en utredning göras i syfte att säkerställa om till exempel information eller data har ändrats eller om någon fiendlig programvara har installerats. Verksamheten ska, med stöd av relevant roll eller funktion såsom till exempel IT, informationssäkerhetssamordnare eller dataskyddsombud, sammanställa och rapportera till säkerhetschefen:

- om det varit ett intrång eller försök till intrång
- om brott mot lagstiftning eller internt regelverk har begåtts
- om incidenten orsakat eller hade kunnat orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång.

Allvarlig informationssäkerhetsincident innebär händelser som kan medföra stor eller katastrofal skada för egen eller annan organisation eller för den enskilde personen.

Allvarliga informationssäkerhetsincidenter ska omgående rapporteras till TIB (tjänsteman i beredskap) och rapporteras till personer som behöver känna till det inträffade såsom säkerhetschef, informationssäkerhetssamordnare, berörd förvaltningens kontaktperson för dataskyddsfrågor och IT-chef.

Dessutom bör detta rapporteras till MSB. Motivet till att rapportera incidenter till MSB är att vi ska bidra till att hjälpa myndigheter, andra kommuner, regioner och företag att upptäcka eventuella trender inom IT-säkerhet samt öka kunskapen kring IT-incidenter generellt.

### **10.3. Rutiner för hantering och rapportering av personuppgiftsincidenter**

En incident kan också innebära att det som inträffat utgör en personuppgiftsincident. Alla personuppgiftsincidenter av allvarlig karaktär ska anmälas inom 72 timmar till Integritetsskyddsmyndigheten, IMY. Incidenter ska hanteras enligt kommunens rutin om personuppgiftsincidenter. Se kommunens intranät för mer information denna typ av incident.

Den som får kännedom om en incident, eller en misstanke om en incident, ska omgående informera sin chef och förvaltningens kontaktperson för dataskyddsfrågor. Verksamheten ska, med stöd av relevant roll eller funktion såsom till exempel IT, informationssäkerhetssamordnare eller dataskyddsombud, sammanställa och rapportera.

## **11. Kontroll**

### **11.1. Kontroll av IT-användning**

För att säkerställa funktion och tillgänglighet till IT-resurser övervakas all användning av kommunkoncernens IT-system. Detta sker genom analys av incidenter och kontinuerlig uppföljning av drift- och säkerhetsloggar. I loggarna registreras exempelvis lyckade och misslyckade inloggningsförsök, viktiga händelser i det aktuella systemet och utloggningar.



Vi kan urskilja vissa filtyper (t ex program-, ljud-, bild- och videofiler). Vid oproportionerligt stora volymer i vår lagring skickas meddelande till användaren/ansvarig. Denne uppmanas rensa eller förklara behovet av extra lagring. Detta behov ska då godkännas av närmaste chef.

All användning av internet loggas med möjlighet att kontrollera vilka webbplatser som besökts. Med hjälp av loggen kan statistik tas fram över de mest besökta webbplatserna. Vid dessa tillfällen sker ingen kontroll av enskilda individers internetanvändning. Om det av statistiken framgår att det förekommer surfing på webbplatser som enligt riktlinjerna inte får besökas, eller om surfing förekommer i onormalt stor omfattning på vissa webbplatser kan arbetsgivaren besluta om kontroll av enskilda individers surfing. Det förs även en logg över all e-post som innefattar uppgifter om avsändare, mottagare, ärendemening och tidpunkt.

Kommunkoncernen kan komma att ta del av de uppgifter som finns i e-postmeddelanden om det är nödvändigt för att uppfylla skyldigheter om allmänna handlingars offentlighet. Observera att detta gäller även vanlig personadresserad post. Kommunkoncernen kan även komma att ta del av de uppgifter som finns i e-postmeddelanden vid fara för informationssäkerheten eller för att utreda och förhindra brott. Uppgifterna som ligger till grund för kontrollen av Internet- och e-postanvändning gallras efter 30 dagar. Om en utredning påbörjas kommer uppgifterna att bevaras så länge utredningen pågår. Misstanke om felaktig eller otillåten användning av gemensamma IT-resurser anmäls till närmaste chef eller politisk organisation som tar ställning till vidare åtgärder.

Arbetsgivaren kommer att agera mot medarbetare som överträder gällande regler och anvisningar genom muntlig tillsägelse, skriftlig varning, omplacering till andra arbetsuppgifter eller i allvarliga fall genom att skilja medarbetaren från anställningen genom uppsägning eller avsked. Vid misstanke om brott sker polisanmälan. Utdrag ur loggar kan komma att utlämnas på begäran från polisen.

## 12. Stöd och hjälp

Vid frågor eller problem angående datorutrustning, programvaror eller liknande, kontaktas IT-Servicedesk.

När det gäller frågor eller problem rörande verksamhetssystem så kontaktas respektive systemförvaltare. Information om vem som är systemförvaltare finns på intranätet under System och program.

Vid frågor rörande hantering av personuppgifter (GDPR) så kontaktas berörd verksamhets kontaktperson alternativt kommunkoncernens dataskyddssamordnare.

Vid frågor rörande informationssäkerhet kontaktas avdelningen för skydd och säkerhet (ASOS).

Vid frågor om informationshantering kontaktas kommunarkivet.

## För mer information

Kristianstads kommun

Martin Ranstorp  
Tel: 044-135445

Linda Perminger  
Tel: 0734- 698105

Linda Söderberg  
Tel: 044-135253

Riktlinjer för informationssäkerhet  
Kristianstads kommunkoncern  
Dnr 2023/534  
Antagen av Kommunstyrelsen  
2023-05-31



Kristianstads  
kommun

| Kristianstads kommun  
Marie Färm | 044-135115  
[www.kristianstad.se](http://www.kristianstad.se) | [kommun@kristianstad.se](mailto:kommun@kristianstad.se)