



Kristianstads
kommun

Kristianstads kommun

Instruktion för digital kommunikation

*Utdrag ur riktlinjer om informationssäkerhet Kristianstads kommunkoncern
beslutad av kommunstyrelsen 2020-03-18.
Gäller fr o m 2020-04-01.*

Innehåll

Inledning	3
Allmänt	3
Mål.....	4
Hantering av informationstillgångar	5
Ansvar.....	5
Offentlighet och sekretess	5
Personuppgifter	5
Personligt ansvar för hantering av all information	6
Personalsäkerhet	6
Rekrytering	6
Anvisningar informationssäkerhet.....	6
Utbildning	6
Användarsäkerhet	7
Allmänna regler	7
Privat användning.....	7
Hem- och distansarbete	8
Lokalt nätverk	8
Externa nätverk.....	8
Digital lagring	9
Behörighet.....	9
Lösenord.....	9
Internet.....	10
E-post.....	10
Snabbmeddelande	11
Datavirus	11
Stöld och sabotage	11
När anställningen upphör.....	11
Incidenthantering	11
Dokumentation av inträffade incidenter	11
Rutiner för hantering av säkerhetsincidenter	12
Rapportering av allvarliga incidenter	12
Kontroll.....	12
Kontroll av IT-användning.....	12
Stöd och hjälp.....	13
Bilagor	13

Inledning

Denna instruktion beskriver det ansvar för informationssäkerheten som vilar på varje användare (medarbetare och förtroendevald) av kommunens nätverk. Digital kommunikation är ett samlingsbegrepp för det som kan utföras med hjälp av olika digitala enheter, såsom dator, mobiltelefon eller surfplatta.

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 kommunledningens viljeinriktning och mål för informations-säkerhetsarbetet 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.

Allmänt

Utgångspunkter för informationssäkerhetsarbetet är:

- lagar, förordningar och föreskrifter
- ISO 27000
- avtal
- våra egna krav.

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 ger inget utrymme för lokala regler som avviker från dessa.

Den som använder kommunens informationstillgångar på ett sätt som strider mot riktlinjerna kan bli föremål för disciplinära åtgärder.

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 möjligt 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 gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- alla investeringar både i form av information och teknisk utrustning skyddas i tillräcklig grad
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.

Hantering av informationstillgångar

Ansvar

Ordinarie verksamhet ansvarar för informationssäkerhet och IT-säkerhet inom sitt verksamhetsområde. Detta styrs i kommunkoncernens säkerhetspolicy. Detta innebär att inom respektive ansvarsområde ansvarar chefer och medarbetare för att upprätthålla rätt nivå av informationssäkerhet samt IT-säkerhet för de processer och resurser de ansvarar för.

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

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 informationssäkerhetsarbetet.

Användare av kommunens IT-system har att följa riktlinjer och instruktioner för informationssäkerhet samt ta del av och följa de regler som finns.

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 diarieföras eller samlas systematiskt så att handlingen kan återsökas. Innehåller en allmän handling sekretessbelagda uppgifter ska handlingen diarieföras.

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.

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.

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.

Personalsäkerhet

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.

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.

Utbildning

Kompetens och medvetenhet är en viktig del i arbetet med informationssäkerhet, framförallt ger den en trygghet för både den anställda och verksamheten.

Alla anställda ska genomföra DISA, 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 anställda.

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.

Användarsäkerhet

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
- det är inte tillåtet att kopiera eller använda programmen utanför kommunkoncernens verksamhet
- vid fel på digital utrustning ska detta omgående anmälas till IT-Service desk
- 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.

Privat användning

Den digitala utrustningen får användas för privat bruk och på ett sådant sätt att arbetet och den digitala utrustningens funktion inte blir lidande eller skadar kommunkoncernens anseende och förtroende. Det är inte heller 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. Alla abonnemang är stängda för utlandssamtal och betaltjänster. Om medarbetarens anställning kräver möjlighet till utlandssamtal kan detta beställas hos IT-avdelningen. Beställning kan även göras för begränsad tid.

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.

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

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.

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.

Digital lagring

När egen information skapas, är det viktigt att veta var den ska lagras. Den information som lagras digitalt på gemensamt lagringsutrymme säkerhetskopieras automatiskt. Här ska information sparas om inget annat meddelats. 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.

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

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.

Lösenord

Vid en anställnings påbörjan tilldelas användaren ett datorkonto med tillhörande lösenord. Detta lösenord kan endast användas vid en första inloggning. När inloggning gjorts ska detta lösenord bytas. 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.

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

E-post

E-post är ett arbetsverktyg, men lagringskapaciteten har begränsats och därför ska gallring göras regelbundet. E-post med bilagor eller länkar kan utgöra ett hot när det gäller spridning av virus. Vid misstanke om oegentligheter öppnas inte bilaga eller länk och kontakt tas med IT-Servicedesk.

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 diarieföring som för vanliga brev
- känsliga personuppgifter och sekretessbelagt material är tillåtet att skickas eller vidarebefordras inom kommunkoncernen, men det ligger på varje förvaltnings och bolags ansvar att avgöra baserat på typ av uppgifter och mottagare
- 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

- 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.

Snabbmeddelande

Skype 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 ej utan rensas bort varje dygn. Det är möjligt att använda dessa verktyg vid kommunikation utanför kommunkoncernens nät, dock med begränsad funktionalitet.

Datavirus

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.

Stöld och sabotage

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

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.

Incidenthantering

Dokumentation av inträffade incidenter

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

Rutiner för hantering av säkerhetsincidenter

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

När en anmälan kommer 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 fientlig 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.

Rapportering av allvarliga incidenter

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 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.

Kontroll

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. Hemkatalogers storlek kontrolleras kontinuerligt då också vissa filtyper kan urskiljas (t ex program-, ljud-, bild- och videofiler). Vid oproportionerligt stor hemkatalog och/eller lagring av större mängder ljud, bild- och videofiler skickas meddelande till användaren. Denne uppmanas rensa sin katalog eller förklara behovet av extra stor katalog. 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 surfning på webbplatser som enligt riktlinjerna inte får besökas, eller om surfning förekommer i onormalt stor omfattning på vissa webbplatser kan arbetsgivaren besluta om kontroll av enskilda individers surfning. 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 90 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.

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.

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

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

Bilagor

Kortversion – Instruktion för digital kommunikation
Ansvarsförbindelse – digital kommunikation

För mer information

Kristianstads kommun

Andreas Poppius
Säkerhetschef
Tel: 0733-135011

Linus Persson
Informationssäkerhetssamordnare
Tel: 0733-135013

Martin Ranstorp
IT-chef
Tel: 044-135445

Rolf Karlsson
HR-strateg
Tel: 044-135522

Utdrag ur riktlinjer om informationssäkerhet
Kristianstads kommunkoncern
Dnr 2020/127



Kristianstads
kommun

| Kristianstads kommun
Rolf Karlsson | 044-135522
www.kristianstad.se | kommun@kristianstad.se