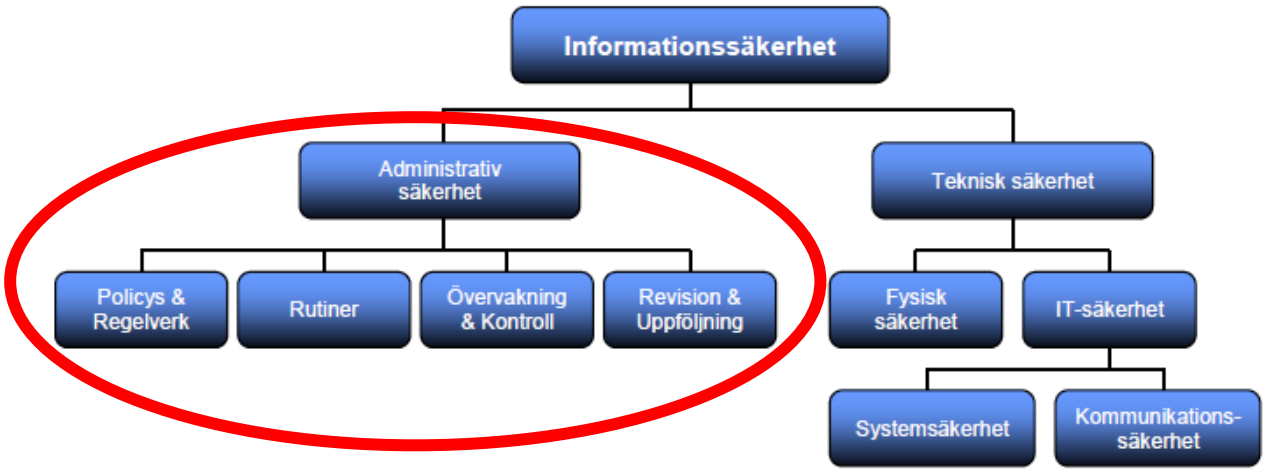
Regelverk för

Informationssäkerhet

Dokumentnamn	**Dokumenttyp**	**Fastställd**	**Beslutsinstans**
Styrande dokument	Plan	2019-06-17 § 78	Kommunfullmäktige
Dokumentansvarig		**Giltig till**	
Kommunstyrelsen		Tills vidare	
Dokumentinformation	Dnr 105/2019		

Informationssäkerhet



Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, hur man fysiskt skyddar utrymmen med dörrar, lås, skåp m.m., eller administrativt i form av regler. Även medarbetares kunskap och medvetenhet är ett nog så viktigt skydd. Säkerhet är aldrig bättre än den svagaste länken.

Den administrativa informationssäkerheten har fokus på människor, medan den tekniska säkerheten har fokus på it och den fysiska på föremål. Det här regelverket handlar till största del om administrativ säkerhet – hur vi ska hantera information i vardagen på säkraste sätt.

Informationssäkerhet är allas ansvar och regelverket gäller samtliga medarbetare i Arvidsjaurs kommun. Enhets- och förvaltningschefer har en utökad skyldighet att se till att medarbetarna känner till regelverket, och att reglerna följs.

Regelverket kompletterar kommunala policys och planer inom informationssäkerhetsområdet, som:

- Informationsplan
- IKT-plan för barn- och utbildningsnämndens verksamheter
- Telefonpolicy SAMSA
- Policy för sociala medier inom Arvidsjaurs kommun
- m.fl.

Det är viktigt att även sätta sig in i och följa dessa policies.

Sist men inte minst måste vi förstås alltid förstå och följa gällande lagstiftning.

Innehåll

Kommunicera

E-post

Din e-post är ett hjälpmedel för att du ska kunna göra ett effektivt jobb. De flesta dokument som du hanterar i tjänsten är allmänna handlingar. Det innebär:

1. Vem som helst har rätt att få insyn i ditt arbete. Insynen gäller även många av dina mejl.
2. Mejl ska sparas och hållas ordnade enligt gällande dokumenthanteringsplan.
3. Vi har e-postregler som är till för att skydda dig, kommunen, och dem vi ger service.

Allmän e-posthandling

- E-post som gäller dina eller kommunens ansvarsområden.
- Bilagor till e-post som gäller dina eller kommunens ansvarsområden.
- Länkar och innehållet i länkar, om det tillför uppgifter till ett ärende.

Inte allmän e-posthandling

- Ojusterade protokoll och liknande handlingar. (De blir allmänna när de justerats.)
- Minnesanteckningar och PM som inte ger ny fakta i ett ärende.
- Utkast till skrivelser, beslut och liknande.
- Privat e-post.

Regler

”Harmlösa” personuppgifter (t.ex. namn och adress) får skickas i mejl. Harmlösa uppgifter är sådana som är allmänt kända och generellt inte kan användas för att orsaka någon skada. I särskilda sammanhang eller tillsammans med andra uppgifter kan harmlösa uppgifter bli skyddsvärda eller känsliga. Tänk på att e-post inte är säkrare än att skicka vykort, så vilken information skulle du själv välja att dela med dig av eller helst hålla hemlig? (Se exempel under regler för Fritextfält)

Sekretessbelagda uppgifter ska inte skickas i mejl, vare sig internt eller externt.

Extra skyddsvärda eller känsliga personuppgifter ska inte skickas i mejl, vare sig internt eller externt.

Sekretessbelagda uppgifter i inkommande mejl:
Socialtjänst, LSS-verksamhet och färdtjänstverksamhet:

- Spara utskrift av mejlet i personakt. Radera sedan mejlet.

Övrig verksamhet:

- Diarieför (om möjligt) mejlet, annars spara det i eget register. Radera sedan mejlet.
  Register ska innehålla:
  - Datum då mejlet kom in.
  - Diarienummer eller annan beteckning.
  - Avsändare eller mottagare.
  - Kort beskrivning av vad mejlet gäller.
  - Mejlet utskrivet på papper eller kopierat till annat dokumentformat (t.ex. Word, Excel, PDF). Förvara ordnat i mapp/pärm eller på datorn.

Extra skyddsvärda eller känsliga personuppgifter i inkommande mejl:

- För in uppgifterna i relevant datasystem, eller
  skriv ut mejlet och spara i mapp/pärm/akt, eller
  kopiera till ett annat dokumentformat (t.ex. Word, Excel, PDF) och förvara ordnat i mapp på datorn.
- Gör en anteckning så att du kommer ihåg vad du gjort. Radera sedan mejlet.

Felsända mejl:

- Vidarebefordra till rätt person eller till kommunens generella brevlåda, kommun@arvidsjaur.se. Radera sedan mejlet.

Övriga mejl:

- Håll ordnade i brevlådan.
- Gallra eller arkivera mejlen enligt dokumenthanteringsplanen.

Sändlistor, kontaktgrupper, massutskick, mejlkopior (cc) o.s.v.:
Det är irriterande att få e-post som inte angår en och överfulla brevlådor är stressande. E-postadresser är också personuppgifter och därför ska vi minimera hanteringen av dem.

- Skicka e-post bara till de som verkligen berörs av innehållet.
- Håll sändlistor och kontaktgrupper uppdaterade så att bara aktuella personer ingår.
- Massutskick ska hållas till ett minimum.
- Massutskick ska ha en utförlig, beskrivande rubrik så att mottagaren lätt kan bedöma innehållets betydelse.

Automatisk vidarekoppling av e-posten till annan adress är inte tillåten.

Intern post

Regler

Sekretessbelagda uppgifter skickas i igenklistrade kuvert.
Extra skyddsvärda och känsliga personuppgifter skickas i igenklistrade kuvert.

För övrig hantering, se Post.

Post

Post är allmänna handlingar på samma bedömningsgrunder som e-post.

Regler

Sekretessbelagda uppgifter i inkommande post:
Socialtjänst, LSS-verksamhet och färdtjänstverksamhet:

- Spara i personakt.

Övrig verksamhet:

- Diarieför (om möjligt) brevet, annars spara det i eget register.
  Register ska innehålla:
  - Datum då brevet kom in.
  - Diarienummer eller annan beteckning.
  - Avsändare eller mottagare.
  - Kort beskrivning av vad brevet gäller.

Förvara ordnat i mapp/pärm.

Övrig post:

- Förvara ordnad i mapp/pärm.
- Gallra eller arkivera breven enligt dokumenthanteringsplanen.

Röstmeddelanden

Röstmeddelanden är allmänna handlingar på samma bedömningsgrunder som e-post.

Regler

Meddelanden som rör ett ärende eller som ska registreras, t.ex. klagomål:

- För in uppgifterna i relevant datasystem, eller
  skriv ner meddelandet och spara i mapp/pärm/akt, eller på datorn.
- Förvara ordnat.
- Gör en anteckning så att du kommer ihåg vad du gjort. Radera sedan meddelandet.

Feladresserade meddelanden:

- Vidarebefordra till rätt person. Radera sedan meddelandet.

Övriga meddelanden:

- Radera när de är inaktuella.

SMS, MMS och liknande meddelanden

SMS, MMS och liknande meddelanden är allmänna handlingar på samma bedömningsgrunder som e-post.

Regler

Sekretessbelagda uppgifter ska inte skickas per telefon eller annan digital tjänst, vare sig internt eller externt.

Extra skyddsvärda eller känsliga personuppgifter ska inte skickas per telefon eller annan digital tjänst, vare sig internt eller externt.

Sekretessbelagda uppgifter i inkommande meddelanden:
Socialtjänst, LSS-verksamhet och färdtjänstverksamhet:

- Spara utskrift/avskrift av meddelandet i personakt. Ange datum, avsändare och medium (SMS, annan tjänst). Radera sedan meddelandet.

Övrig verksamhet:

- Diarieför (om möjligt) meddelandet, annars spara det i eget register. Radera sedan meddelandet.
  Register ska innehålla:
  - Datum då meddelandet kom in.
  - Diarienummer eller annan beteckning.
  - Avsändare eller mottagare.
  - Kort beskrivning av vad meddelandet gäller.
  - Meddelandet utskrivet/avskrivet på papper eller kopierat till annat dokumentformat (t.ex. JPG, PNG). Förvara ordnat i mapp/pärm eller på datorn.

Extra skyddsvärda eller känsliga personuppgifter i inkommande meddelanden:

- För in uppgifterna i relevant datasystem, eller
  skriv ut/skriv av meddelandet och spara i mapp/pärm/akt, eller
  kopiera till ett annat dokumentformat (t.ex. JPG, PNG) och förvara ordnat i mapp på datorn.
- Gör en anteckning så att du kommer ihåg vad du gjort. Radera sedan meddelandet.

Meddelanden som rör ett ärende eller som ska registreras, t.ex. klagomål:

- För in uppgifterna i relevant datasystem, eller
  skriv ut/skriv av meddelandet och spara i mapp/pärm/akt, eller
  kopiera till ett annat dokumentformat (t.ex. JPG, PNG) och förvara ordnat i mapp på datorn.
- Gör en anteckning så att du kommer ihåg vad du gjort. Radera sedan meddelandet.

Övriga meddelanden:

- Håll ordnade i brevlådan.
- Gallra eller arkivera meddelandena enligt dokumenthanteringsplanen.

Publicera

Hemsida

Visionen för kommunens hemsida är att den ska vara den första och bästa kommunikationskanalen för medborgare och besökare. För att vi ska nå dit måste sidan vara objektiv, tillförlitlig, uppdaterad och användbar. Innehållet ska följa gällande lagar, förordningar, och kommunens policys.

Regler

Reglerna gäller för hemsidan och även för länkade sidor.

Sekretessbelagda uppgifter ska inte publiceras på hemsidan.

Extra skyddsvärda eller känsliga personuppgifter ska inte publiceras på hemsidan.

”Harmlösa” personuppgifter får inte publiceras om uppgifterna, enskilt eller tillsammans med andra uppgifter, kan leda till att den personliga integriteten kränks.

Foton på personer ska som regel publiceras med skriftligt samtycke. Blankett finns i mappen ”Allmänna kommunmallar”. Foton på barn under 18 år kräver vårdnadshavarnas samtycke.
I dessa fall kan du publicera utan samtycke:

- Det finns en annan rättslig grund för publiceringen, t.ex. att det är av allmänt intresse att en viss information sprids. Fråga GDPR-samordnaren eller informatören.
- Bilder på anställda och politiker i offentliga roller, d.v.s. främst högre chefer och de som jobbar direkt mot allmänheten. Det är dock god hyfs att fråga först.
- Personer som inte kan identifieras (t.ex. står med ryggen mot kameran).
- Döda personer.

Foton och bilder med upphovsrätt får inte publiceras utan skriftligt tillstånd från fotografen (upphovsmakaren) eller köpta publiceringsrättigheter.

Följ informatörens anvisningar för språk, textupplägg, grafisk profil, länkning, citering o.s.v.

Facebook och andra sociala medier

Vi har ett ansvar för det material som publiceras på sociala medier som Facebook, LinkedIn, Twitter, YouTube, Flickr och bloggar. Ansvaret gäller både det vi själva lägger ut och inlägg av besökare. Inläggen är generellt allmänna handlingar.

Regler

Reglerna gäller för det sociala mediet och även för länkade sidor.

Alla verksamheter ska rapportera sina konton i sociala medier till informatören.
Informatören:

- Hjälper till att bedöma om mediet är lämpligt för det tänkta syftet.
- Ger anvisningar för informationstext, språk, textupplägg, länkning o.s.v.
- För ett register över kommunens närvaro i sociala medier.

Sekretessbelagda uppgifter ska inte publiceras i sociala medier.

Extra skyddsvärda eller känsliga personuppgifter ska inte publiceras i sociala medier.

”Harmlösa” personuppgifter får inte publiceras om uppgifterna, enskilt eller tillsammans med andra uppgifter kan leda till att den personliga integriteten kränks.

Sekretessbelagda uppgifter i inlägg av besökare:
Socialtjänst, LSS-verksamhet och färdtjänstverksamhet:

- Spara utskrift av inlägget i personakt.
- Skicka om möjligt ett direktmeddelande till besökaren och förklara att du tar bort kommentaren och varför. Hänvisa till våra regler för inlägg som ska finnas under ”Om” på alla kommunens sidor. (Finns i samling med informationstexter. Fråga kommunikatören.)
- Radera inlägget.
- Skriv i kommentarsfältet att de inlägg som inte följer våra regler tas bort. Hänvisa till reglerna som ska finnas under ”Om” på alla kommunens sidor.
- Gör en anteckning så att du kommer ihåg vad du gjort.

Övrig verksamhet:

- Diarieför (om möjligt) inlägget, annars spara det i eget register. Register ska innehålla:
  - Datum då inlägget gjordes.
  - Diarienummer eller annan beteckning.
  - Avsändare.
  - Kort beskrivning av vad inlägget gäller.
  - Inlägget utskrivet på papper eller kopierat till annat dokumentformat (t.ex. Word, Excel, PDF). Förvara ordnat i mapp/pärm eller på datorn.
- Skicka om möjligt ett direktmeddelande till besökaren och förklara att du tar bort kommentaren och varför. Hänvisa till våra regler för inlägg som ska finnas under ”Om” på alla kommunens sidor.
- Radera inlägget.
- Skriv i kommentarsfältet att de inlägg som inte följer våra regler tas bort. Hänvisa till reglerna som ska finnas under ”Om” på alla kommunens sidor.
- Gör en anteckning så att du kommer ihåg vad du gjort.

Extra skyddsvärda eller känsliga personuppgifter i inlägg av besökare;
Direkta personuppgifter i inlägg av besökare som enskilt eller tillsammans med indirekta uppgifter kan kränka någons personliga integritet;
Brottsliga inlägg av besökare:

- För in uppgifterna i relevant datasystem, eller
  skriv ut inlägget och spara i mapp/pärm/akt, eller
  kopiera till ett annat dokumentformat (t.ex. Word, Excel, PDF) och förvara ordnat i mapp på datorn.
- Skicka om möjligt ett direktmeddelande till besökaren och förklara att du tar bort kommentaren och varför. Hänvisa till våra regler för inlägg som ska finnas under ”Om” på alla kommunens sidor.
- Radera inlägget.
- Skriv i kommentarsfältet att de inlägg som inte följer våra regler tas bort. Hänvisa till reglerna som ska finnas under ”Om” på alla kommunens sidor.
- Gör en anteckning så att du kommer ihåg vad du gjort.

Foton på personer ska som regel publiceras med skriftligt samtycke. Blankett finns i mappen ”Allmänna kommunmallar”. Foton på barn under 18 år kräver vårdnadshavarens samtycke.
I dessa fall kan du publicera utan samtycke:

- Det finns en annan rättslig grund för publiceringen, t.ex. att det är av allmänt intresse att en viss information sprids. Fråga GDPR-samordnaren eller informatören.
- Bilder på anställda och politiker i offentliga roller, d.v.s. främst högre chefer och de som jobbar direkt mot allmänheten. Det är dock god hyfs att fråga först.
- Personer som inte kan identifieras (t.ex. står med ryggen mot kameran).
- Döda personer.

Foton och bilder med upphovsrätt får inte publiceras utan skriftligt tillstånd från fotografen (upphovsmakaren) eller köpta publiceringsrättigheter.

Enskilda ärenden ska inte hanteras via sociala medier.

- Be besökare som gjort inlägg i enskilt ärende att ta direktkontakt genom brev, e-post, telefonsamtal, eller personligt besök.
- Spara en kopia av inlägget tillsammans med övriga handlingar som skapas i ärendet.

Råd eller upplysningar som kan få ekonomiska konsekvenser ska inte ges i sociala medier.
Vi kan bli skadeståndsskyldiga om vi lämnar felaktiga uppgifter.

Privata konton

Mejlen och telefonnumret du har i arbetet får inte användas i det privata.

Sekretessbelagda uppgifter som du tagit del av i arbetet är sekretessbelagda även när du agerar som privatperson.

Uttala dig inte för kommunens räkning via ditt privata konto. Tydliggör att du uttalar dig som privatperson.

Foton på kolleger tagna i arbetsrelaterade sammanhang ska endast publiceras med samtycke.

Kommunens logotyp får inte användas i det privata.

Videosändning, öppen

Säg att du anordnar ett öppet event (utbildning, konferens, föreläsning el. likn.) och sänder det via webben, direkt och/eller inspelat. Eftersom röst och bild är personuppgifter måste du informera alla deltagare om att sändningen är öppen och vad du gör med inspelningen efteråt. Det gör du lättast direkt på anmälningsblanketten. Mall på den information som måste finnas med hittar du i mappen ”Allmänna kommunmallar”. Du måste också ha skriftligt samtycke från eventuella fysiska deltagare som kommer att visas i bild. Samtyckesblankett finns också i mappen ”Allmänna kommunmallar”.

Ger du möjlighet för deltagare att ställa frågor via mikrofon under eventet så måste du informera om att röstupptagningen blir en del av sändningen. Väljer deltagare då att tala så har du konkludent samtycke till upptagningen, d.v.s. personerna samtycker genom sitt handlande.

Skydda

Dator

Datorer är arbetsverktyg. Det du gör på datorn loggas och det du sparar är arbetsgivarens material. Det allra mesta är allmänna handlingar. Datorn står i direkt kontakt med kommunens interna nät. Eftersom vi lagrar mycket sekretessbelagd information och uppgifter som av olika anledningar ska skyddas mot obehörigt intrång måste vi hantera datorerna på ett säkert sätt.

Regler

Lås datorn när den lämnas utan uppsikt.

Spara dokument i din personliga hemkatalog (H:), eller i en gruppenhet (t.ex. I:), inte på den lokala hårddisken (C:) eller på skrivbordet**.** IT tar säkerhetskopior på alla filer som sparas i hemkatalogerna. På datorns lokala hårddisk och skrivbordet har du ingen backup. Den som gör intrång i datorn kan se dina filer och filerna försvinner med datorn om den kraschar eller installeras om.

Spara inte dokument i onödan, särskilt inte sådana som innehåller personuppgifter. Gallra eller arkivera i enlighet med dokumenthanteringsplanen.

Nedladdning/lagring av programvaror, appar och filer från okända eller tvivelaktiga webbplatser/e-postmeddelanden är inte tillåtet. Virus finns oftast på internet i bilder, filer och gratisprogram men smittan kan också komma i e-post och då framför allt i e-postbilagor.

Datorn bör inte användas i privata syften. Sammanställningar över användningen, t.ex. webbhistorik och andra logguppgifter är allmänna handlingar.

Misstänker du att någon gjort intrång i din dator ska du genast anmäla det till IT och till GDPR-huvudsamordnaren.

System och programvaror

Förvaltningschef, alternativt enhetschef, är per automatik systemägare till de datasystem och programvaror som förvaltningen/enheten skaffat och/eller är huvudanvändare av. Systemägaren kan utse en eller flera systemförvaltare som ska sköta systemen och kontakterna med leverantörer. IT-avdelningen ger en del teknisk support och står i vissa fall för drift av system.

Regler

System och programvaror ska upphandlas enligt LOU.

System och programvaror ska minst möta lagens krav på informationssäkerhet.

Systemägare ansvarar för att användare utbildas i aktuella system. Utbildningar ska inkludera både de generella regler som finns i det här regelverket (behörighet, fritextfält, skyddsvärda, känsliga och sekretessbelagda uppgifter o.s.v.) och specifika regler som gäller för systemet eller förvaltningen.

Systembehörighet

Alla anställda ges elektronisk tillgång till uppgifter och system som de behöver för sitt arbete. Behovet av åtkomst varierar beroende på verksamhetsområde och den anställdes arbetsuppgifter. För att begränsa den elektroniska tillgången har vi ett system för behörighetsstyrning.

Regler

Ansvarig chef beställer, korrigerar och avslutar behörighet för varje enskild användare.

Användaruppgifter är personliga och får inte lämnas ut. Användaridentiteten tillsammans med lösenordet identifierar dig när du använder datasystemen. Du är ansvarig för allt som händer ”i ditt namn”.

Använd inte samma användarnamn eller lösenord vid registreringar utanför kommunens system som i kommunens system. Om en extern webbplats hackas så kan det ge åtkomst till kommunens nätverk.

Automatisk minnesfunktion för lösenord ska inte användas. Låt inte webbläsare spara lösenordet när du loggar in på en webbplats. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/lösenord, som kan användas om man är osäker på om lösenord har lagrats.

Lösenord ska bytas regelbundet. Det är rekommenderat att byta lösenordet några gånger om året.

Använd olika lösenord privat och i jobbet.

Fritextfält, anteckningar, kommentarer i system

De flesta av de datasystem som vi använder erbjuder möjligheten att skriva kommentarer och anteckningar i fritext, alltså med egna ord. Det är viktigt att det som skrivs i fritext inte kan upplevas som kränkande av individen, dels för att det går emot vår värdegrund och dels för att texten kan komma att lämnas ut i registerutdrag eller som allmän handling enligt offentlighetsprincipen.

Regler

Fritextfält ska bara utnyttjas om det är absolut nödvändigt.

Sekretessbelagd information ska inte noteras i fritext.

Extra skyddsvärda eller känsliga personuppgifter får endast noteras i fritext:

- **med personens skriftliga samtycke; eller**
- **om det är nödvändigt för att fullgöra våra skyldigheter inom arbetsrätt, social trygghet, eller socialt skydd;**
- **om personen själv tydligt har offentliggjort uppgifterna;**
- **om det är nödvändigt med hänsyn till ett viktigt allmänt intresse;**
- **om det är nödvändigt för att ge lagstadgad hälso- och sjukvård samt social omsorg, eller för att bedöma arbetstagares arbetskapacitet.**

Som alternativ till att notera känsliga uppgifter kan man exempelvis skriva ”Frånvarande” istället för ”Sjukskriven”, eller ”Fackansluten” istället för ”Medlem i Kommunal” o.s.v.

Skriv inte något som du själv skulle uppleva som kränkande om noteringen gällde dig.

Noteringar ska vara omedelbart nödvändiga. En uppgift som kanske kan komma till användning eller vara bra att ha i framtiden, men inte behövs för ett aktuellt ärende, ska inte noteras.

Noteringar ska vara relevanta. Att någon är ensamstående med tre barn kan vara relevant för en ansökan om bostadsbidrag, men inte nödvändigtvis för en ansökan om bygglov.

Noteringar ska vara objektiva och sakliga. Det är skillnad mellan att skriva att någon ”gormade och betedde sig som en idiot” och att någon ”var upprörd”.

Skilj på värderingar av prestationer och värderingar av personliga egenskaper, beteenden eller attityder.

- Prestationer kan värderas objektivt utifrån uppgift och mål.
- Omdömen om personliga egenskaper, beteenden eller attityder är subjektiva och präglade av personkemi och dina egna normer.

Koder ska inte användas i fritext. Koder betyder exakt det man internt har kommit överens om att de betyder. Om det exempelvis står ”*#!!” i kod så är det lika kränkande som att i klartext skriva ”han ljuger”. Dessutom måste alla koder förklaras om en person begär ett registerutdrag.

Undvik att notera uppgifter om tredje personer som du anger med namn. Det kan exempelvis räcka att skriva ”Gift” snarare än ”Gift med Ola Persson”.

Jobbmobil, laptop, padda och andra mobila enheter

Mobiltelefonen och andra mobila arbetsverktyg som du har tillgång till i tjänsten innehåller uppgifter som är allmänna handlingar. En mobil enhet som används i arbetet och som kan kopplas upp mot våra interna nät kan användas för attacker in i organisationen om den kommer i orätta händer. Eftersom vi lagrar mycket sekretessbelagd information och uppgifter som av olika anledningar ska skyddas mot obehörigt intrång måste vi hantera de mobila enheterna på ett säkert sätt.

Regler

Mobila enheter ska vara lösenordskyddade.

Lås mobila enheter som lämnas utan uppsikt.

Kontaktuppgifter till privatpersoner

- Kontaktuppgifter till privatpersoner sparas bara om uppgifterna är absolut nödvändiga för ett aktuellt ärende.
- Spara inte fler uppgifter än som behövs. Sekretessbelagda, extra skyddsvärda eller känsliga uppgifter ska inte sparas alls.
- Radera kontaktuppgifterna så snart ett ärende är avslutat.

Foton

- Foton på privatpersoner kräver samtycke för att få användas. Blankett finns i mappen ”Allmänna kommunmallar”.
- Flytta foton från mobila enheter till relevant datasystem eller mapp/pärm/akt så fort som möjligt. Radera kopior i den mobila enheten**.**

Meddelanden från okända avsändare

- Öppna inte meddelanden från okända avsändare.
- Klicka inte på länkar som skickats från okända personer/avsändare.
- Avaktivera automatisk öppning av bilagor.

Molntjänster ska användas i minimal utsträckning. Det är svårt att kontrollera om säkerhetsåtgärderna för tjänsterna är tillräckliga och information i molntjänster lagras i många fall på servrar i länder utanför EU. Om informationen innehåller personuppgifter så innebär det en olaglig överföring till tredje land. Ladda endast ned molntjänster från stora, kända leverantörer. Tänk på att du själv ansvarar för applikationer som inte godkänts av din arbetsgivare.

Begränsa nedladdningen av appar. Använd endast appar från stora, kända leverantörer, med många tidigare nedladdningar och med okontroversiellt innehåll. Tänk på att du själv ansvarar för applikationer som inte godkänts av din arbetsgivare.

Molntjänster och appar ska inte ha tillgång till uppgifter som kontakter, foton eller din position.

Stäng av de tjänster du inte behöver för tillfället, t.ex. WLAN, Bluetooth, GPS, och datatrafik. Det minskar enhetens exponering.

Mobila enheter bör inte användas i privata syften. Sammanställningar över användningen, t.ex. webbhistorik och andra logguppgifter är allmänna handlingar.

Mobila enheter ska som regel lämnas på arbetet vid dagens slut, om du inte har avtalat något annat med din chef.

Misstänker du att någon gjort intrång i din mobila enhet ska du anmäla det till IT direkt.

Privata mobila enheter

Privata mobila enheter ska inte användas för arbetsrelaterade uppgifter.

Jobbmejl, kalender, kontakter o.s.v. ska inte synkroniseras till privata mobila enheter.

USB-minnen

Regler

USB-minnen och andra flyttbara lagringsmedia ska skyddas med exempelvis lösenord och ska inte lämnas utan uppsikt.

Okända flyttbara lagringsmedia kan innehålla virus och ska användas med försiktighet.

Papper, pärmar, lappar och mappar

Vi producerar många handlingar i pappersform, allt från post it-lappar till rapporter. Stora delar är allmänna handlingar. Ibland finns sekretessbelagd information, eller extra skyddsvärda alternativt känsliga personuppgifter i handlingarna. Det innebär att informationen måste hållas ordnad och skyddas på olika sätt.

Regler

Sekretessbelagd information och extra skyddsvärda eller känsliga personuppgifter ska hållas under uppsikt. Lås in handlingarna eller lås kontoret när du lämnar det.

Spara inte fler handlingar än nödvändigt.

- Kopior och ”bra att ha”-grejer är oftast inte nödvändiga.
- Utskrifter på information som finns i datasystem eller på sådant som kan läsas på nätet är oftast inte nödvändiga.

Gallra eller arkivera handlingar enligt dokumenthanteringsplanen.

- Sekretessbelagd information och handlingar som innehåller personuppgifter ska tuggas i dokumentförstörare eller på annat sätt göras oläsliga.

Besökare, konsulter, leverantörer…

Många utomstående personer rör sig i kommunens lokaler varje dag, som reparatörer, hantverkare, konsulter, och leverantörer. Det är trevligt med besökare och gäster av olika slag, men eftersom vi hanterar stora mängder sekretessbelagd och känslig information så måste vi tänka till innan vi ger dem tillträde till våra kontor eller datasystem.

Regler

Besökare som har möjlighet att röra sig fritt i våra lokaler eller ges tillgång till sekretessbelagd eller känslig information ska underteckna ett sekretessavtal. Det gäller inte de som redan är bundna av sekretess genom sin profession eller genom särskilda klausuler i tjänsteavtal.

Besökares inloggning till datasystem ska fungera under begränsad tid.

Sekretessbelagd och känslig information ska låsas in inför besök på ditt kontor.

Incidenter och incidentrapportering

En incident inträffar om information på något sätt:

- blir förstörd
- går förlorad på annat sätt
- kommer i orätta händer

Det spelar ingen roll om händelsen sker oavsiktligt eller med avsikt.

Exempel:

- En mobiltelefon blir stulen.
- En dator kraschar och information som lagrats lokalt kan inte återskapas.
- Personuppgifter skickas till någon som inte skulle ha uppgifterna.
- En anställd får tillgång till data som inte behövs för arbetsuppdraget.
- En person som slutat sin tjänst fortsätter att ha tillgång till kommunens system.
- Ett nätfel stänger ner ett system så att lagstadgad service inte kan levereras.
- Det sker ett intrång på kommunens servrar.

En informationssäkerhetsincident kan få allvarliga följder och ska inte ignoreras.

Regler

Fysisk incident där personuppgifter är inblandade ska omedelbart anmälas till GDPR-huvudsamordnaren. Exempel: Papper som försvinner, utskrifter som glöms i skrivaren, personer som snokar i pärmar på kontor.

Digital incident där personuppgifter och teknik (dator, mobil o.s.v.) är inblandade ska omedelbart anmälas till GDPR-huvudsamordnaren och IT-enheten. Exempel: Mobiltelefon blir stulen, virus infekterar en dator, mejl med personuppgifter skickas till fel mottagare.

Fysisk incident där opersonlig information (information utan personuppgifter) är inblandad ska omedelbart anmälas till förvaltningschef.

Digital incident där opersonlig information och teknik (dator, mobil o.s.v.) är inblandad ska omedelbart anmälas till förvaltningschef och IT-enheten.

För chefer gäller även instruktioner i dokumentet ”GDPR - Anvisningar för chefer”.

Förklaringar

Allmän handling

Tryckfrihetsförordning (1949:105)

2 kap. 3-8 §

- Handlingar är alla skrifter, bilder och inspelningar som kan läsas, avlyssnas eller uppfattas med tekniska hjälpmedel.
- Handlingar är allmänna, om de har kommit in till kommunen, skapats i kommunen, förvaras hos kommunen, eller verkställts av kommunen.

2 kap. 12-13 §

- Allmän handling som får lämnas ut ska lämnas ut så snart det är möjligt. Handlingen ska kunna läsas, avlyssnas eller på annat sätt uppfattas.
- Är delar av handlingen sekretessbelagd ska övriga delar lämnas ut.
- Den som begär en handling har generellt rätt att vara anonym.
- Behöver vi pröva om det finns hinder för att handlingen lämnas ut (sekretessprövning) får vi fråga efter identitet och syftet med begäran.

Vad är inte en allmän handling?

2 kap. 9-11 §

- Minnesanteckningar, kladdar, övertaliga kopior och post it-lappar som inte tillför ett ärende något;
- Utkast till skrivelser eller beslut som inte verkställts;
- Säkerhetskopior av datasystem;
- Privata handlingar

Dokumenten blir likafullt allmän handling om de registreras eller tas om hand för arkivering.

Brottsligt, exempel

Tryckfrihetsförordning (1949:105)

1 kap. 10 § Barnpornografi

7 kap. 4 § Uppvigling, hets mot folkgrupp, olaga hot, olaga våldsskildring, förtal, förolämpning, hot mot tjänsteman, övergrepp i rättssak.

Yttrandefrihetsgrundlag (1991:1469)

5 kap. 1 § Det som är tryckfrihetsbrott enligt Tryckfrihetsförordning 7 kap. 4-5 § är också yttrandefrihetsbrott. Dessutom är skildring av grovt våld mot människor eller djur olagligt.

Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk

1 kap. 1 § Upphovsrätten gäller

1. skönlitterär eller beskrivande framställning i skrift eller tal (inkl. kartor, teckningar och grafik),
2. datorprogram,
3. musikaliskt eller sceniskt verk,
4. filmverk,
5. fotografiskt verk eller något annat alster av bildkonst,
6. alster av byggnadskonst eller brukskonst, eller
7. verk som har kommit till uttryck på något annat sätt.

Sekretessbelagda uppgifter

Offentlighets- och sekretesslag (2009:400)

Sekretess = tystnadsplikt. Det innebär att en sekretessbelagd uppgift inte får röjas, varken skriftligen eller muntligen.

17 kap. Sekretess för inspektion, kontroll eller annan tillsyn
18 kap. Sekretess för, t.ex.:
- Skyddade identiteter
- Säkerhets- eller bevakningsåtgärder
- Risk- och sårbarhetsanalyser, krishanteringsplaner

19 kap. Sekretess för, t.ex.:
- Myndighets affärsverksamhet
- Upphandling
- Fackliga förhandlingar

21 kap. Sekretess för uppgift om enskilds personliga förhållanden, t.ex.:
- Hälsa och sexualliv
- Personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med Allmänna dataskyddsförordningen (GDPR)
  (Generellt är det dock tillåtet att lämna ut personuppgifter i allmänna handlingar.)

22 kap. Sekretess i folkbokföring, delgivning, m.m.
23 kap. Sekretess i utbildningsverksamhet, m.m.
26 kap. Sekretess inom socialtjänst, vid kommunal bostadsförmedling, adoption, m.m.
28 kap. Sekretess när det gäller socialförsäkringar, studiestöd, arbetsmarknad, m.m.
32 kap. Sekretess som rör annan tillsyn, granskning, övervakning, m.m., t.ex.:
- Överförmyndare

39 kap. Sekretess i personaladministrativ verksamhet
40 kap. Sekretess i övriga verksamheter, t.ex.:
- Val
- Bibliotek
- Växeltelefonister

Extra skyddsvärda och känsliga personuppgifter

Allmänna dataskyddsförordningen (EU) 2016/679 (GDPR)

5 art. Personuppgifter får behandlas men:

- De ska behandlas på laglig grund, korrekt och öppet.
- Bara de uppgifter som verkligen behövs ska behandlas.
- Uppgifterna ska inte förvaras längre tid än vad som är nödvändigt för behandlingen.
- Organisatoriska och tekniska skydd ska finnas på plats för att säkra personuppgifterna.

Extra skyddsvärda personuppgifter

- Uppgifter om barn (Skäl 38)
- Uppgifter om lagöverträdelser och brott (10 art.)
- Personnummer och samordningsnummer (Dataskyddslag 3 kap. 10 §)
- Uppgifter om person eller privatliv (Skäl 75), t.ex.:
  - Omdömen
  - Arbetsprestationer
  - Personlig ekonomi (inkomst, skatt, skuld etc.)

Känsliga personuppgifter

9 art. Känsliga personuppgifter som får behandlas bara om det är absolut nödvändigt, eller om individen själv tydligt offentliggjort uppgifterna.

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska och biometriska uppgifter
- Uppgifter om hälsa
- Sexualliv och sexuell läggning

”Harmlösa” personuppgifter, exempel

- Namn
- Befattning
- E-postadress till arbete
- Telefonnummer till arbete
- Födelsedatum (alltså utan de fyra sista siffrorna)
- Registreringsnummer på fordon
- Fastighetsbeteckning
