MARIESTAD

Rutin informationssäkerhet

Mariestad

MARIESTAD

Antaget av Kommunens ledningsgrupp

Mariestad
2017-12-11

MARIESTAD

Datum: 2017-12-11

1 Informationssäkerhet

Information är en av kommunens viktigaste tillgångar och är avgörande för en fungerande verksamhet. Den finns i många olika former, exempelvis i pappersdokument, digitala verksamhetssystem och i medarbetarnas medvetanden. Arbetet med informationssäkerhet syftar till att information ska hållas hemlig för obehöriga, att den finns tillgänglig när den behövs samt att informationen ska vara riktig.

Detta dokument redovisar hur du som medarbetare och förtroendevald ska verka för att upprätthålla en god informationssäkerhet. Även om det i rutinen genomgående skrivs medarbetare så gäller den även för förtroendevalda (i tillämpliga delar).

Yttrandefriheten och tryckfriheten garanteras av våra grundlagar och ger alla människor i Sverige rätten att i princip fritt utrycka sig i tal och skrift. I två av våra grundlagar slås dessutom fast att anställda i en kommunal myndighet får överlämna sekretessbelagda uppgifter till massmedia för publicering, det så kallad meddelarskyddet. Det är uppgifterna som får lämnas över, det är däremot inte tillåtet att lämna över själva handlingen som innehåller de sekretessbelagda uppgifterna. Undantaget från meddelarskyddet är de uppgifter som omfattas av tystnadsplikten, dessa får inte överlämnas till massmedia för publicering. Vad som är en tystnadspliktig uppgift framgår i Offentlighets- och sekretesslagen.[1] Avsiktlig spridning av sekretessbelagda uppgifter i annat syfte än ovan samt oavsiktlig spridning är däremot inte tillåtet.

2 Ansvar för medarbetare och chefer

För att uppnå en god informationssäkerhet krävs säkerhetsmedvetande hos alla som hanterar informationen, utrustning (dator, telefon, surfplatta) och inpasseringsenheter. Att känna till och följa denna rutin följer av anställningen. Vid nyanställning ska närmaste chef säkerställa att medarbetaren läser och förstår denna rutin. Det ska ske innan åtkomst ges till kommunens nätverk (KIS).

Vissa verksamheter har utöver dessa regler även verksamhetsspecifika sådana. Närmaste chef ska känna till om så är fallet.

Även tillfällig medarbetare eller konsulter eller andra externa samarbetsorganisationer omfattas av samma regler som övriga medarbetare. Den som anlitar sådana aktörer ansvarar för att de också tar del av detta regelverk.

De som kommer i kontakt med uppgifter som kan vara sekretessbelagda ska känna till vilka särskilda regler som gäller för denna typ av information.

[1] Se intranätet för mer information http://navet.mariestad.se/anstallning-och-arbetsmiljo/sakerhet_krishantering/Sidor/Informationssäkerhet.aspx

Särskilt ansvar för personer i chefsposition

Alla i chefsposition har enligt denna rutin ett antal särskilda uppgifter. I ett separat dokument beskrivs dessa uppgifter mer ingående. Dokumentet ligger på intranätet.

3 Stöd i informationssäkerhetsarbetet

Om du har frågor kring informationssäkerhet så vänd dig till din närmaste chef eller kommunens säkerhetssamordnare. Om du har frågor eller problem gällande kommunens nätverk (KIS) eller kommunövergripande system såsom epost så vänd dig till IT-support. Vad gäller verksamhetssystem vänd dig till systemansvarig i verksamheten.

Information om informationssäkerhetsfrågor finns på intranätet som du når genom att klicka på denna länk. Mer information finns också på exempelvis www.informationssakerhet.se

4 Inloggning och lösenord

För att få tillgång till kommunens nätverk (KIS) och olika verksamhetssystem krävs inloggning. Olika verksamhetssystem ställer olika höga krav på säkerhet i inloggning. Vissa medarbetare behöver exempelvis använda mobilt bankID eller andra särskilda autenticeringsmetoder för att logga in i system.

Val av lösenord till olika verksamhetssystem är systemspecifikt. Den i verksamheten som är ansvarig för systemet kan ge mer information. Till vissa verksamhetssystem ges tillgång direkt via inloggningen till kommunens nätverk (KIS).

Dina lösenord är strängt personliga och ska hanteras därefter. Du själv kan bli misstänkt om någon använder din behörighet för olämpliga ändamål. Du ska därför:

- aldrig avslöja eller ”låna ut” ditt lösenord,
- skydda lösenordet väl, inte skriva ner det på papper eller spara på plats där andra kan komma åt det,
- omedelbart byta lösenord om du misstänker att någon kan känna till det,
- aldrig använda samma lösenord för flera system.

Lösenord blir generellt sett starkare - svårare att gissa - ju längre det är.

5 Dator, telefon, surfplatta och inpasseringsenheter

Du ansvarar för att hantera din utrustning på ett säkerhetsmedvetet sätt. Det innebär exempelvis att skydda den från stöld samt att hantera den varsamt för att undvika skada. Det är bara kommunanställda som får använda utrustningen.

Vid behov av ny utrustning ska närmaste chef kontaktas för godkännande av beställning. Gammal utrustning ska alltid återlämnas.

Dator

IT-avdelningen ansvarar för att datorn innehåller ett visst säkerhetsskydd (t.ex. programvara till skydd mot skadlig kod). Det ger endast visst skydd – ditt eget beteende är ofta avgörande.

Dator ska regelbundet anslutas till kommunens nätverk (KIS) så att dokument och filer säkerhetskopieras. Då görs också viktiga säkerhetsuppdateringar. Vid misstanke att du drabbats av virus eller annan form av skadlig kod så stäng genast av datorn och kontakta IT-support. Logga heller inte in på en annan dator då koden kan finnas i din hemkatalog och ”väckas till liv” om du loggar in på annan dator. Det är viktigt föra att begränsa risken att koden sprider sig i kommunens nätverk.

Om du misstänker att en dator som delas av flera personer drabbats av virus eller annan form av skadlig kod gäller samma tillvägagångssätt som ovan. Stäng genast av datorn och kontakta IT-support. Meddela också kollegorna att datorn inte får sättas på.

Installation av programvaror och konfiguration av datorn ska utföras av IT-avdelningen för att skapa en så säker IT-miljö som möjligt. Vissa typer av program kan dock rent tekniskt installeras utan IT-avdelningens hjälp. Det får dock inte göras utan tillåtelse från närmaste chef.

Vid tillfällen när du inte har uppsikt över dator ska den låsas. Det görs enkelt genom att trycka tangenterna ctrl, alt, delete och sedan trycka enter.

Mobiltelefon

PIN-kod eller annan form av autentisering (t.ex. fingeravtryck eller grafiskt skärmlås) ska alltid vara aktiverad. Vissa verksamheter där telefoner delas mellan flera medarbetare kan behöva undantas från kravet på PIN-kod eller personlig autentisering. Chef för verksamheten ska i så fall fatta beslut om det.

Iaktta försiktighet vid nedladdning av appar till telefonen. Många appar kräver omfattande åtkomsträttigheter för att kunna installeras (t.ex. kontaktlista, position, meddelanden och foton). Om du hanterar information med höga krav på konfidentialitet i din telefon bör appar för privat bruk därför inte laddas ner. Det är inte tillåtet att ladda ner appar som inte finns i App Store eller Google Play.

Ibland får du ett meddelande i telefonen om att det finns systemuppdateringar att installera. Det är viktigt att dessa installeras eftersom de bland annat åtgärdar upptäckta säkerhetsproblem. Om du inte har tillräcklig surfmängd så kontakta din närmaste chef för att öka upp den.

Surfplatta

Samma regler som gäller för dator gäller också för surfplattor.

Extern lagringsutrustning

Du bör vara restriktiv med att lagra information på extern lagringsutrustning som exempelvis USB-minne eller extern hårddisk. Information som ändå lagras på sådant sätt ska då också lagras i hemkatalog eller gemensam filyta för att automatisk säkerhetskopiering ska ske. Flyttbara enheter ska förvaras och hanteras på ett säkerhetsmedvetet sätt, bland annat att skydda utrustningen från stöld och från att obehöriga använder den.

Information med höga krav på konfidentialitet får inte lagras på flyttbara enheter. Undantag kan göras för rutiner som syftar till att säkerställa verksamhetens fortsatta arbete även vid bortfall av verksamhetssystem. Enheten ska krypteras eller förvaras i låst utrymme. Kryptering görs genom att koppla in enheten, öppna utforskaren, högerklicka på enheten, välja ”aktivera bitlocker” och sedan följa instruktionerna på skärmen. Ring IT-support vid behov av hjälp.

Det är inte tillåtet att ansluta okända USB-minnen till datorn, t.ex. USB-minnen du hittat eller fått av okänd person/organisation. Det inkluderar tillfällen när personer från andra organisationer med hjälp av USB-minne föra över information till dig. Även om du litar på personen ifråga kan du inte veta att USB-minnet inte innehåller någon form av skadlig kod. Be personen att istället maila över information. Om epostsystemet hänvisar till att filen är för stor så kan du kontakta IT-support och be dem temporärt öka den tillåtna storleken på bifogade filer. Om det är absolut nödvändigt och det kan antas att den som har USB-minnet behandlat det säkert så får det användas.

Reglerna ovan för USB-minnen gäller också minneskort och CD-ROM-skivor samt andra eventuella liknande lagringsmedia.

Inpassering

Kommunen har ett antal olika system för inpassering i fastigheter. Både traditionella nycklar och olika elektroniska lösningar (exempelvis tags).

Den inpasseringsenhet du fått är värdefull och ska hanteras så att de inte går förlorade. Om obehörig person kommer över den kan de få tillgång till kommunens lokaler och den information som finns däri. Förlust av inpasseringsenhet ska omedelbart anmälas så att den kan spärras (för elektroniska enheter) eller att traditionella lås vid behov bytas ut.

Förlust av utrustning eller inpasseringsenhet

IT-support ska kontaktas vid förlust av dator och surfplatta. De säkerställer då att enheten inte kan anslutas till kommunens nätverk (KIS) för att komma åt information.

Vid förlust av telefon ska du kontakta den du fick enheten av. Den ska spärras samt om möjligt fjärraderas för att säkerställa att ingen kommer åt information i enheten. Om du inte vet hur fjärradering görs så kontakta IT-support.

Vid förlust av inpasseringsenhet anmäls det till den person/funktion som lämnade ut den.

Alla stölder av dator, telefon, surfplatta eller liknande ska polisanmälas. Samråd sker mellan medarbetare och närmaste chef om vem som gör anmälan.

6 Distansarbete

Din närmaste chef beslutar om du ska ges möjlighet att arbeta på distans. Vid distansarbete ansvarar du för att den utrustning du eventuellt använder:

- Ges lämpligt fysiskt skydd för att förhindra stöld, brand etc,
- skyddas mot obehörig insyn,
- skyddas mot obehörig användning,

Vid anslutning till okända wifi-nätverk finns risken att någon avlyssnar all trafik. Det innebär att mail kan läsas och inloggningsuppgifter i olika verksamhetssystem kan stjälas. Om du behöver ansluta till andra nätverk än kommunens ska du därför, så långt det är praktiskt möjligt, försäkra dig om att nätverket är säkert. Det är exempelvis tillåtet att ansluta sig till tågbolagets nätverk, att ansluta sig till nätverk på konferensanläggningar och hotell samt andra nätverk som rimligen är säkra. Det är däremot inte tillåtet att ansluta sig till okända nätverk. Använd uppkoppling via din tjänstetelefon om det inte finns säkra nätverk eller om du är osäker på om ett nätverk är säkert. Kontakta närmaste chef om du behöver höja upp din surfmängd.

Det är inte tillåtet att från arbetsplatsen ta med information i fysisk form med höga krav på konfidentialitet om den lämnas utan uppsikt. Det är exempelvis tillåtet att ta med papper till ett möte när du lämnar arbetsplatsen men inte att förvara känslig information hemma eller på annan plats.

7 Hantering av information

Klassificering av information

Alla kommunens informationstillgångar ska vara klassade efter hur viktigt det är att tillgången hålls konfidentiell, tillgänglig och riktig. Viss information har mycket höga krav på konfidentialitet, exempelvis uppgifter om skolelevers hälsa. Annan information kan ha höga krav på tillgänglighet, såsom styrsystem för el- eller dricksvattenförsörjning, medan riktighet är särskilt viktigt för exempelvis journalsystem inom vård och omsorg.

Kraven på hur informationen får hanteras beror på resultatet av klassificeringen.

Det finns mer att läsa om informationklassificering på intranätet samt i det stöddokument för chefer som tidigare nämnts.

Behandling av personuppgifter

Med behandling menas allt man gör med personuppgifter, exempelvis insamling, registrering, lagring, bearbetning och spridning. För att det ska vara tillåtet att behandla personuppgifter måste det finnas en rättslig grund. Personuppgiftslagen (som 25 maj 2018 ersätts av dataskyddslagen) innehåller en rad olika rättsliga grunder som gör det tillåtet att behandla personuppgifter, något som ju ofta är nödvändigt för att kunna bedriva kommunal verksamhet av olika slag. Vid frågor om behandling av personuppgifter kontakta närmaste chef.

Lagring av information

Information kan finnas lagrad i olika former. Den kan finnas i fysisk form på papper, i digitala verksamhetssystem och i medarbetarnas medvetande. Oavsett på vilket sätt den är lagrad så ska den behandlas på lämpligt sätt. Resultatet av informationsklassificeringen ska visa vilka säkerhetsåtgärder som är lämpliga.

Digital lagring

Du ska inte lagra viktig information lokalt på din dator, telefon eller surfplatta eftersom den förloras om enheten går sönder eller försvinner. Information ska istället lagras i hemkatalog eller gemensam lagringsyta. Alternativt i ett för verksamheten avsett dokument- och ärendehanteringssystem eller annat verksamhetssystem.

Sekretessbelagd information får inte skickas med epost eller SMS. Om du tar emot sekretessbelagd information via dessa kanaler ska den överföras till en säker förvaring och sedan raderas från epost, telefon etc.

Molnbaserade lagringstjänster

Uppgifter med höga krav på konfidentialitet får lagras i molntjänst endast om en särskild risk- och sårbarhetsanalys genomförts samt om ett antal säkerhetsåtgärder vidtagits. Personuppgifter får lagras i molntjänst endast om en särskild utredning är genomförd och personuppgiftsbiträdesavtal upprättats med tjänsteleverantören. Beslut om detta måste tas av ansvarig politisk nämnd/styrelse.

Vid minsta osäkerhet om det är tillåtet att lagra viss information i en molnbaserad tjänst – stäm av med din närmaste chef.

Information i fysisk form

Skriftligt material som innehåller information med höga krav på konfidentialitet får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i när man lämnar arbetsplatsen.

Vid utskrift av information med höga krav på konfidentialitet ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen.

Det är inte tillåtet att från arbetsplatsen ta med den typen av information i fysisk form om den lämnas utan uppsikt. Det är exempelvis tillåtet att ta med papper till ett möte när du lämnar arbetsplatsen men det är inte tillåtet att förvara informationen hemma eller på annan plats än arbetsplatsen.

Pappersdokument som innehåller denna typ av information får inte kastas i pappersinsamling. De måste strimlas eller kastas i godkända säkerhetskärl.

Fax

Försök undvika att använda fax för att skicka information med höga krav på konfidentialitet. Om det ändå måste göras ska man försäkra sig om att man har rätt nummer (t.ex. använda sig av kortnummer) och att mottagarens fax är övervakad av rätt mottagare under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.

När information med höga krav på konfidentialitet ska mottas via fax – be avsändaren ringa innan sändningen görs så att du kan övervaka faxen när dokumentet kommer. Om faxen har en digital brevlåda behöver denna procedur så klart inte göras.

Övrig hantering av information

Information med höga krav på konfidentialitet har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan ta del av sådan information, oavsett om det är på eller utanför arbetsplatsen.

Vid samtal där sådan information tas upp ska du försäkra dig om att ingen annan kan höra. Be en kollega om hjälp med att kontrollera om det går att höra samtal på ditt kontor/mötesrum genom väggar/dörr.

Kontrollera också om det är lätt att se in på ditt kontor. Går det exempelvis att genom fönsterruta på markplan se din skärm eller dokument på ditt kontor? Säkerställ i så fall att det finns insynsskydd på fönstret. Om det finns insyn till din arbetsplats bör datorer inte lämnas på skrivbordet pga inbrottsrisk. En bärbar dator kan istället läggas i en låda eller annan dold plats.

Se också ”Riktlinjer för dokumenthantering” för andra regler om hantering av information, t.ex. gallring och diarieföring.[2]

8 Användning av Internet

Användning av Internet ska ske inom de ramar som sätts upp av lagar och förordningar. Vid misstanke om brott samarbetar arbetsgivaren med polismyndigheten.

Hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet. Undantag kan göras om sådan hantering behövs för att utföra arbetsuppgifter. Det ska godkännas av närmaste chef.

Undvik att besöka sidor som kan antas kunna sprida skadlig kod. Undvik också att ladda ner filer från sidor som du inte till fullo litar på.

Se kapitlet om distansarbete för regler om anslutning till andra nätverk än kommunens.

9 Användning av e-post

E-postmeddelande omfattas av samma offentlighets-, sekretess- och arkivregler som gäller för övrig post. Den enskilda medarbetaren som är kontoinnehavare är ansvarig för den e-post som skickas från kontot. I ansvaret ligger också att kontrollera sin e-post. Vid semester eller annan längre frånvaro utses någon annan som läser inkommande e-post. Ett alternativ är att ha ett autosvar som tydligt anger en annan e-postadress som det går bra att skicka e-posten till.

---

[2] http://navet.mariestad.se/nyheter/Sidor/Riktlinjer-för-dokumenthantering.aspx

Närmaste chef beslutar om medarbetare ska få tillgång till varandras brevlådor. Använd gärna funktionsbrevlådor som kan kopplas till flera användare för att öka tillgängligheten.

Nedan följer ett antal regler för användning av e-post:

- Det är inte tillåtet att uppträda under annans namn då e-postsystemet används.
- Det är inte tillåtet att skicka sekretessbelagd information med e-post.
- Var restriktiv med att använda e-postadressen för privat bruk.
- Var eftertänksam när du uppger din e-postadress på Internet. Det kan leda till att du får ta emot spammeddelanden och liknande.
- Var noggrann när du adresserar e-postmeddelande så att det går till rätt person. Om du får ett feladresserat e-postmeddelande bör du informera avsändaren samt radera meddelandet.

Bedrägligt beteende via e-post

Det är mycket vanligt att e-post används för att sprida skadlig kod eller för att lura mottagaren. Därför är det viktigt att vara på sin vakt när man använder e-posten.

Öppna inte bifogade filer till epostmeddelanden från okända avsändare. Var även försiktig med att öppna filer från kända avsändare om du inte väntar dig att få en bifogad fil. Vid osäkerhet är det lättaste att höra av sig till avsändaren och säkerställa den bifogade filens riktighet.

Klicka heller inte på länkar som finns i mail från okända avsändare.

Det är vanligt med falsk e-post från någon som utger sig för att vara en viss person eller organisation, t.ex. banker, myndigheter eller någon inom den egna kommunen. Om du är osäker på om ett mail är äkta eller inte finns olika sätt att gå tillväga. Du kan kontakta avsändaren, låta en kollega kolla på mailet eller kontakta IT-support.

10 Informationssäkerhetsincidenter

En informationssäkerhetsincident är en händelse som kan få negativa konsekvenser för en informationstillgångs konfidentialitet, riktighet eller tillgänglighet. Det kan t.ex. vara misstanke om virus, intrång i IT-system, förlust av utrustning, förlust av information i fysisk form eller i verksamhetssystem, att känslig information sprids till obehörig eller obehörig användning av din användaridentitet.

Det är viktigt att alla säkerhetsincidenter rapporteras, stora som små. En säkerhetsincident behöver inte ge negativ påverkan omedelbart men kan med tiden få större konsekvenser och leda till värre incidenter. Rapportera både incidenter som drabbat eller rör dig själv men också sådant som du noterar i din omgivning.

Informationssäkerhetsincidenter ska rapporteras så snart som möjligt. De rapporteras alltid till närmaste chef, på samma sätt som är fallet vid andra typer av incidenter. Om incidenten innebär gäller utrustning eller IT-system kontaktas också IT-support. Vid misstanke att du drabbats av virus eller annan form av skadlig kod så stäng genast av datorn och kontakta IT-support. Logga heller inte in på en annan dator då koden kan finnas i din hemkatalog och ”väckas till liv” om du loggar in på annan dator. Det är viktigt föra att begränsa risken att koden sprider sig i kommunens nätverk.

Det är tillåtet att rapportera incidenter anonymt. Det kan exempelvis göras genom att skriva ner incidenten, lägga papperet i ett kuvert med din närmaste chefs namn på och lägga i dennes brevlåda.

Om du anser att organisationer eller personer utanför kommunens verksamhet inte hanterar information på ett säkert sätt så bör du upplysa dem om det.

Rapporteringens syfte är inte att skuldbelägga någon utan att begränsa konsekvenser av incidenten och ge möjlighet att lära av händelsen så att det inte händer igen.

11 Avslutad eller ändrad anställning

När du slutar din anställning ansvarar du för att:

- Återlämna utrustning du tilldelats av kommunen, t.ex. dator, telefon, surfplatta och externa lagring.
- Säkerställ att det inte finns arbetsrelaterad information lagrad på privat dator eller telefon samt att du inte har sådan information i fysisk form hemma hos dig.
- Rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas.

När du byter anställning är det viktigt att dina behörigheter anpassas till den nya tjänsten. Det kan innebära att du får tillgång till nya verksamhetssystem, att behörigheter för andra system försvinner med mera.

12 Ordlista

Begrepp	Förklaring
Autentisering	Verifiering av att en användare eller IT-resurs är den som den utger sig för att vara.
Behörighet	Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt.
Gemensamma lagringsytor	Vanligtvis en mapp på KIS som flera användare har tillgång till. Kan också ligga på Onedrive om verksamheten använder Office 365.
Hemkatalog	Dina filer och systeminställningar ligger här. Exempelvis information du sparar på skrivbordet och i mina dokument
Informationklassificering	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Informationstillgång	Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t.ex. rykte).
Konfidentialitet	Information är endast tillgänglig för dem som är behöriga att ta del av den.
Känsliga personuppgifter	Uppgifter som enligt personuppgiftslagen omfattas av ett särskilt skydd. Det är information som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv.
Information med höga krav på konfidentialitet	All information som kan vara belagd med sekretess. Därutöver information som om den sprids kan leda till omfattande negativa konsekvenser. Typiskt sett information som i informationsklassificering nått nivå 2-3.
Molntjänst	Tjänst som tillhandahålls över Internet, framförallt lagring av information samt vissa andra funktioner. Exempelvis Dropbox, Google Drive och iCloud.
Riktighet	Informationen skyddas mot oönskad och obehörig förändring eller förstörelse.
Skadlig kod	Program som används för att obehörigen skaffa tillgång till information eller störa en organisations verksamhetssystem/IT-miljö. Exempelvis virus, trojaner och ransomware.
Spårbarhet	Ändringar av information är möjlig att följa i efterhand.

Tillgänglighet	Informationen finns tillgänglig enligt verksamhetens krav.
Tvåfaktorautentisering	Verifiering i två steg av att en användare är den som den utger sig för att vara. Kräver exempelvis både inloggning med ett lösenord samt en engångskod som skickas via SMS. Eller inloggning med kod i kombination med ett särskilt identifikationskort som stoppas in i datorn.
Verksamhetssystem	Program som är specifikt för viss verksamhet och som ofta har en systemförvaltare i verksamheten. Exempelvis sociala system som Procapita, pedagogiska system och industriella styrsystem.