Rutiner för hantering av information

Beslutsinstans:	Kommundirektör
Beslutsdatum:	2014-11-24
Giltighetstid:	Tillsvidare

Dokumentet **" Styrdokument för informationssäkerhet"** och **"Riktlinjer för informationssäkerhet"** är kopplat till dessa rutiner och anger de övergripande målen för informationssäkerheten.

Godkänd
2014-11-24
Åsa Heribertson

Åsa Heribertson
kommundirektör

Innehåll

1. Inledning

Du som medarbetare är den enskilt viktigaste länken i arbetet för en god informationssäkerhet. Det är därför viktigt att du själv är aktiv i att ta reda på vilka regelverk som gäller för din arbetsplats.

Syftet med detta dokument är att ge tydliga beskrivningar i hur man som anställd i Danderyds kommun övergripande ska hantera information. Dokumentet beskriver även hur man ska hantera information i mobila enheter som bärbara datorer, läsplattor och smarta telefoner.

För att öka säkerhetsmedvetandet ska alla som arbetar i Danderyds kommun genomgå en introduktionsutbildning inom informationssäkerhet. Denna ges i samband med introduktionsutbildningen för nyanställda. För att bibehålla en hög nivå på säkerhetsmedvetandet ska regelbunden och relevant informationssäkerhetsutbildning genomföras för de som arbetar inom Danderyds kommun.
Det som står beskrivet i rutinbeskrivningen gäller alla sorters information såsom information i pärmar, på skrivbord, i samtal och digital information, e-post, internet, dokument sparade i nätverksmappar.

Alla användare har ett ansvar för att informationen som Danderyds kommun hanterar är av hög kvalité. Den ska vara tillgänglig, riktig, spårbar och när det finns skäl för det, hanteras enligt bedömd sekretessnivå.

Detta dokument kompletterar Styrdokument för informationssäkerhet 2011-2014 samt Riktlinjer för informationssäkerhet.

2. Klassificering av information

Klassning av en organisations information utgör en av grunderna för att skapa en effektiv informationssäkerhet. Klassificeringen delar in informationen i olika informationsklasser. Klasserna beskriver hur informationen får hanteras, lagras, distribueras och avvecklas. Klassificering av information görs på systemnivå av systemförvaltarna.

3. Lösenordshantering

Målet med regler för lösenordshantering är att förhindra obehörig åtkomst till kommunens utrustning och information. Det betyder att Danderyd kommuns behöriga användare ska vara medvetna om sitt ansvar gällande åtkomst till information, då särskilt när det gäller användning av lösenord och säkerhet för användarutrustning.

Lösenord ska användas för åtkomst till samtliga system i verksamheten. Lösenord ska även användas för privat utrustning som används i tjänsten för t.ex. synkning av e-post.

Läsplattor och smarta telefoner ska förses med lösenord eller s.k. Touch ID (fingeravtrycksläsare).

4. E-post och Internet

4.1 E-post

Avsnittet syftar till att säkerställa hantering av inkommande och utgående e-post till och från Danderyds kommun och även hanteringen av information som inkommer och skickas via mobila enheter.

Generellt gäller:

1. Sekretessbelagd eller på annat sätt känslig information ska inte skickas via e-post. Tänk på att e-post kan komma på avvägar eller på annat sätt bli läst.
2. Massutskick kan uppfattas som skräppost av e-postsystemet och bör därför göras med försiktighet.
3. Kommunens e-post system får inte användas för egen kommersiell eller ideell verksamhet

Danderyds kommuns personal ska inte e-posta känsliga uppgifter vare sig internt eller externt. Känsliga uppgifter är sådana uppgifter som den enskilda individen kan lida men av om uppgiften sprids.

Inkommen e-post med känsliga uppgifter ska inte vidarebefordras. Om informationen behöver föras vidare ska den skrivas ut.

4.2 Internet

Syftet med rutinen är att ge vägledning och instruktioner vid användning av internet inom Danderyds kommun.

Internet är ett värdefullt hjälpmedel som ger tillgång till mängder av information. Internet kan alltså vara ett stöd för att göra ett bra arbete. Det finns dock vissa risker med användningen av internet. Olämplig användning av internet kan skada Danderyd Kommuns namn och rykte. Sådan skada kan också drabba enskilda medarbetare. En felaktig användning av internet kan vidare skada eller förstöra lagrad information på kommunens datorer och servrar.
Varje medarbetares goda omdöme och ansvarsfulla inställning är viktig för att undvika att organisationen eller någon medarbetare på något sätt skadas av felaktig användning av de tjänster internet erbjuder.

Tänk på att du alltid uppträder i tjänsten då du använder en uppkoppling till internet. Det finns inget som hindrar att du efter arbetstidens slut eller på raster använder Danderyd Kommuns internet-uppkoppling för att söka efter information för privat bruk. Läs dock noga de begränsningar som anges nedan.
All internetaktivitet från kommunens nätverk sparas i form av loggar. Loggarna kan användas vid misstanke om brott eller för att spåra regelöverträdelser.

4.2.1 Olämpliga webbsidor

Varje medarbetare förväntas hantera Danderyds Kommuns uppkoppling mot internet på ett etiskt korrekt sätt. En användare får inte koppla upp sig mot webbsidor, e-

postgrupper, diskussions-grupper, chattsidor eller liknande som har – eller kan misstänkas ha – olämpligt eller stötande innehåll till exempel kränkningar på grund av kön, etnisk eller religiös tillhörighet, brott mot mänskliga rättigheter, pornografi, kriminell verksamhet eller annan olämplig information. Detta gäller inte om du behöver ha tillgång till sådana sidor i tjänsten.

4.2.2 Ladda ner programvaror och filer

Det är inte tillåtet att utan tillstånd ladda ner *programvaror* till dator eller server. Okända program kan innehålla virus. De skador som kan orsakas av en sådan felaktig hantering kan bli betydande, både interna servrar och programvaror kan skadas allvarligt. Nedladdning av program kan också innebära brott mot licens- och copyrightregler.

Nedladdning av *filer* med icke arbetsrelaterat material bör ske med försiktighet. Det finns risk för att man begår olagligheter eftersom det kan handla om material som är skyddat av upphovsrätten.

4.3 Virus och skräppost (spam)

På all utrustning som tillhandahålls av kommunen finns skydd mot virusangrepp och skräppost. Dessa skydd uppdateras kontinuerligt. Det kan trots detta hända att vi drabbas av virusangrepp eller skräppost.

4.3.1 Virus

Datorvirus är små datorprogram som sprider sig genom att lägga en kopia av sig själva inuti andra program, *värdprogram*, på sådant sätt att koden körs då värdprogrammet körs. Då ett infekterat värdprogram körs kan dess virus spridas ytterligare och även utföra annat som viruset har konstruerats för att göra. I dagligt tal kallar man ofta alla typer av skadlig programkod för virus.
För att ett virus ska kunna infektera en dator eller sprida sig måste du vanligen göra något, t.ex. öppna en infekterad e-postbilaga eller klicka på en länk i ett e-post meddelande.

Virus eller skadlig kod kan finnas i/på:

- Hemsidor, även sådana som verkar seriösa. Detta kan dock vara svårt att undvika.
- Bakom bilder i ett mail, i social medier, på internet och särskilt i skräppost (spam).
- I bilagor och i länkar som du får via e-post.
- I nedladdning av program.
- USB-minnen, CD-skivor eller instickskort.

4.3.2 Skräppost

Skräppost är oönskad post som skickas till din e-postadress där avsändaren på något sätt försöker tjäna pengar genom reklamutskick eller bedrägerier. Det kan även vara post där du uppmanas att ange kontonummer eller lösenord. Sådan e-post ska aldrig besvaras.

Råd för att undvika skräppost:

- Lämna inte ut din e-postadress på webbplatser eller diskussionsforum.
- När du får skräppost i din brevlåda är den bästa åtgärden att radera de oönskade breven utan att öppna dem.
- Svara inte på skräppost. Genom att svara bekräftar du att din adress finns och används.

4.4 Molntjänster

Vi liksom andra har tillgång till ett växande antal molntjänster. Innan det kan bli aktuellt att använda sådana måste ett antal överväganden göras som handlar om informationssäkerhet. Det går inte att i dokument som detta precisera vad som gäller angående molntjänster då området är stadd i en snabb utveckling. Därför ska alltid innan en molntjänst tas i bruk kontakt tas med kommunens säkerhetschef för en bedömning om risker, hot och möjligheter. Innan beslut fattas ska kommunens IT-forum konsulteras. Beslut fattas därefter av förvaltningschef.
Organisationen Cloud Sweden har tagit fram ett dokument som belyser området molntjänster: *Riktlinjer – Områden och problem att beakta inom informationssäkerhet och digitalt bevarande vid anskaffning och användning av molntjänster.*

5. Arkiv och dokumenthantering

Här hänvisas till de dokumenthanteringsplaner som finns för respektive nämnd och styrelse.
Vid tveksamheter kontakta kommunens arkivchef.

6. Publicering av information

Det som sägs här angående publicering av information gäller för all publicering på webben inklusive i sociala medier.
Vid publicering av klassificerad information följer klassningen av informationen med till andra system.
Vi som anställda hanterar information där det är viktigt att tänka på integritetsaspekten och att därför inte utan medgivande publicera bilder och personuppgifter.

7. Mobila enheter

Det finns stora likheter mellan hanteringen av mobila enheter och hanteringen av bärbara datorer. Fysisk förvaring och uppkoppling är två områden där hanteringen ser likadan ut. Det finns också många områden där hanteringen skiljer sig åt exempelvis inloggning och säkerhetsuppdateringar för att nämna några.
Nedan följer beskrivningar som gäller särskilt för mobila enheter. Det som sagts tidigare i denna rutinbeskrivning gäller även för hantering av mobila enheter.

7.1 Användaren ska kvittera ut den mobila enheten

Användaren ska kvittera ut den mobila enheten för att visa att man tagit del av de regler som gäller.

7.2 Uppkoppling

Många mobila enheter är utrustade med 3G- eller 4G-abonnemang för ständig åtkomst till internet. Trådlös nätverksuppkoppling är möjlig i en del kommunala lokaler. Finns tillgång till trådlöst nätverk även i hemmet är det lämpligt att använda detta på grund av ökad prestanda. Detta supporteras inte av Danderyds kommun utan du ansvarar själv för uppkopplingen i hemmet.

7.3 Vilka tjänster som får användas

Utöver de programvaror (appar) som du behöver i tjänsten ansvarar du själv för de program som installeras på den mobila enheten. Du ska inte låta appar nyttja kontaktboken då detta kan resultera i att innehållet i kontaktboken kan missbrukas.

7.4 Ominstallation och överlåtelse

All ominstallation och överlåtelse till ny användare ska gå via IT-avdelningen.

7.5 Förvaring av mobila enheter

Kommunen har ingen försäkring som kan användas vid förlust/skada av den mobila enheten.
Användaren ska hantera och förvara den mobila enheten på ett sätt så att skada och stöld förebyggs. Ersättningsskyldighet kan uppkomma vid vårdslös hantering.

Vid förlust av sin mobila enhet ska omedelbart IT-avdelningen kontaktas.
Polisanmälan görs av användaren.

7.6 Radera information som inte längre behövs (regelbundet)

Radering av information som inte längre behövs i den mobila enheten ska göras regelbundet av användaren så att den mobila enheten innehåller så lite information som möjligt för att minimera informationsläckage vid förlust.

7.7 Säkerhetsuppdateringar

Ansvaret för att göra de säkerhetsuppdateringar av mobilens operativsystem och applikationer som krävs ligger på dig som användare. När en säkerhetsuppdatering kommer till telefonen och du får meddelande om detta ska du acceptera och installera säkerhetsuppdateringen. Säkerhetsuppdateringar skyddar mobilen och dess applikationer mot nya hot och svagheter och det är därför viktigt att de blir installerade snarast.

7.8 Virus eller skadlig kod i mobila enheter

Vid misstanke om att den mobila enheten smittats av virus eller skadlig kod skall IT-avdelningen kontaktas för närmare besked hur det ska åtgärdas.

8. Uppföljning

- Denna rutin ska informeras om för nyanställda och vara en del av introduktionsprogrammet.
- Respektive chef ansvarar för att ta upp rutinen i sina arbetsgrupper för diskussion regelbundet.
- Säkerhetschefen är huvudansvarig för denna rutin.
- Vid frågor om denna rutinbeskrivning, kontakta närmaste chef.