Riktlinjer för informationssäkerhet

Beslutsinstans:	Kommundirektör
Beslutsdatum:	2013-02-26
Giltighetstid:	Tillsvidare
Riktlinjerna har behandlats i förvaltningschefsgruppen den 21 februari 2013. Dokumentet **" Styrdokument för informationssäkerhet"** är kopplat till dessa riktlinjer och anger de övergripande målen för informationssäkerheten.	

1 Inledning

1.1 Syfte

Det antagna dokumentet Styrdokument för informationssäkerhet beskriver den politiska ledningens *vilja* med informationssäkerheten. Syftet med riktlinjerna är att beskriva de övergripande målen i styrdokumentet och *vad* som ska göras för att nå målen.

1.2 Omfattning

Detta dokument, riktlinjer för informationssäkerhet, innehåller de riktlinjer som gäller för hantering av såväl information som informationsbärare i form av datorer, pappersdokument, mobiltelefoner och externa minnen etc. Information kan finnas lagrad eller hanteras i digital form, men kan också vara i såväl skriftlig som muntlig form. I detta dokument är informationsbäraren inte det viktiga, men i dagens organisation hanteras informationen mest i digital form och därför har dokumentet en tyngdpunkt mot datorer och dess information.

1.3 Avgränsning

Detta regelverk beskriver den informationssäkerhet som ska gälla vid arbete med information, system och program inom Danderyds kommun.

Detta regelverk gäller såväl anställda som inhyrd och kontrakterad personal inom Danderyds kommun. Regelverket gäller även de som på uppdrag av kommunen fått tillgång till Danderyds kommuns information och informationssystem.

2 Nyckelbegrepp

All information som hanteras eller lagras i någon form måste skyddas mot oönskad förändring, påverkan eller insyn. Det ska inte heller vara möjligt för obehöriga att ta del av information och de användare som har rätt till informationen ska komma åt den efter behov och inom önskad tid. Det är också av vikt att kunna identifiera vem som har gjort vad med informationen.

Därför kan området informationssäkerhet delas in i följande fyra egenskaper

Riktighet
Att information inte kan förändras vare sig obehörigen, av misstag eller på grund av tekniska störningar. Informationen ska vara tillförlitlig, korrekt och fullständig.

Sekretess
Att dokumentation, information och handlingar etc. inte görs tillgängliga eller avslöjas för obehörig.

Spårbarhet
Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt- användare, skrivare, dator eller system/program. Det ska gå att se vem som tagit del av informationen, vilka förändringar som har gjorts och av vem

dessa har utförts.

Tillgänglighet
Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

3 Struktur för säkerhetsdokumentation

I *styrdokument för informationssäkerhet* fastställer kommunfullmäktige sin syn på informationssäkerhet, övergripande mål och intention med informationssäkerhetsarbetet.

Riktlinjerna för informationssäkerhet beskriver vilka rutiner och säkerhetslösningar som måste etableras, för att uppfylla de mål som beskrivs i styrdokumentet för informationssäkerhet. Riktlinjerna syftar inte till att detaljerat beskriva hur rutiner och säkerhetslösningar i praktiken ska utformas, utan ger en minsta förväntad nivå för dessa. Detta för att dels etablera en gemensam säkerhetsnivå som alltid måste uppnås, dels för att rutiner och säkerhetslösningar ska kunna anpassas till verksamhetens normala rutiner och sätt att arbeta.

Utifrån detta upprättas *rutinbeskrivningar*, som detaljerat redogör för hur rutiner och säkerhetslösningar ska utformas och tillämpas, för att informationssäkerhetspolicyns krav ska efterlevas.

Övriga dokument relaterade till styrning och användning av IT inom Danderyds kommun utgörs av:

- **Riktlinjer för IT**: beskriver IT-miljön inom Danderyds kommun och krav på tekniska system. Dokumentet är främst avsett att användas som underlag i design, upphandling med mera
- **Systemförvaltningsmodell**: beskriver roller och ansvar kring förvaltning av kommunens IT-system. Riktad till dem som har en roll inom förvaltningen av kommunens IT-miljö.

Kommunens informationshantering styrs främst av bestämmelser i tryckfrihetsförordningen, Offentlighet - och Sekretesslagen (OSL) (2009:400) samt arkivlagen. Huvudregeln i tryckfrihetsförordningen är att information ska vara tillgänglig för allmänheten, den s.k. offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i OSL kan omfattas av sekretesskydd samt information inom överförmyndarverksamheten. Det är väsentligt att varje anställd känner till vilken information, inom i första hand sitt eget ansvarsområde, som är sekretessbelagd och hur den ska hanteras. Prövning av sekretess föreligger för informationen varje gång en begäran av utlämning sker. Detta oavsett om handlingen är sekretessbelagd eller inte.

Kommunen bör också följa riktlinjer kring IT-verksamheten samt informationshantering från SKL (Sveriges kommuner och landsting), kammarkollegiet, MSB (Myndigheten för samhällsskydd och beredskap), KSL (kommunförbundet Stockholms län) och andra kommungemensamma intresseorganisationer. Som exempel kan nämnas rekommendationen 16 principer för samverkan från KSL och som bl a Danderyds kommun ställt sig bakom.

Vid motsägelser gäller regelverken i följande ordning

1) Lagar och förordningar
2) Styrdokument för informationssäkerhet

3) Riktlinjer för informationssäkerhet

4 Kontinuitetshantering

Kontinuitetshantering fokuserar på att:

- säkerställa att i första hand samhällskritiska processer ska kunna fungera på en acceptabel nivå vid svåra störningar,
- avbrutna ordinarie processer ska kunna återupptas inom en acceptabel tidsrymd under vilken alternativa rutiner upprätthåller prioriterad, kritisk verksamhet,
- säkra verksamheten vid olika typer av risker,
- lägga ansvaret för åtgärder (återhämtningsrutiner mm.) på den som "äger" den samhällskritiska resursen.

Kontinuitetshantering syftar alltså till att säkerställa rutiner för att minimera avbrott i kommunens verksamheter. Alla system och verksamheter har risker. En riskanalys ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta system samt identifiera och analysera skyddsvärda verksamheter och kritiska områden inom kommunen. Kommunens förvaltning och bolag ska inventera, analysera, värdera, förebygga och åtgärda oönskade händelser inom sina ansvarsområden. Arbetet ska fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, information och egendom/verksamhet.

En analys ska omfatta:

- Vilken verksamhet som måste fungera oavsett påfrestningar och vilka system som stöder denna verksamhet.
- Vilka system som säkerställer att kärnvärdena uppfylls – både organisatoriska och tekniska system samt sårbarheten i dessa system.
- Tänkbara risker och hot som på ett avgörande sätt kan utmana förmågan att upprätthålla den kommunala servicen samt sannolikheten för att de inträffar.

De risker som identifieras ska hanteras. Detta görs genom att:

- Genomföra åtgärder som minskar riskerna till en acceptabel nivå.
- Acceptera riskerna om de inte strider mot lagstiftning eller kommunens regler.
- Undvika den aktivitet som orsakar att den identifierade risken blir verklighet.
- Överföra risken till andra parter, tex försäkringsbolag eller leverantörer.

5 Säkerhetsorganisation – roller och ansvar

5.1 Allmänt

För att uppnå och bibehålla fastställda regler för informationssäkerhet krävs en tydlig ansvarsfördelning inom organisationen samt att säkerhetsarbetet koordineras.

5.2 Kommunstyrelsen

Kommunstyrelsen har ansvar för att se till att det finns en väl fungerande organisation för informationssäkerhetsarbetet. Kommunstyrelsen ska initiera och stödja säkerhetsarbetet med resurser.

5.3 Kommundirektör

Kommundirektören är på kommunstyrelsens uppdrag ansvarig för efterlevnaden av styrdokument för informationssäkerhet. Kommundirektören fastställer dessa riktlinjer för informationssäkerhet. Kommundirektören utser informationssäkerhetschef.

5.4 Säkerhetschef

Säkerhetschefen har det yttersta säkerhetsansvaret inom Danderyds kommun.
I korthet omfattar ansvaret för säkerhetschefen att:

- Ansvara för kommunens färdriktning i långsiktiga, strategiska IT- och informationssäkerhetsfrågor.
- Utforma regelverk för informationssäkerhet och uppdatera dessa vid behov.
- Upprätta former för kontinuitetshantering, riskanalys och incidenthantering.
- Utvärdera säkerhetsnivån inom kommunen.
- Hantera allvarliga säkerhetsincidenter.

5.5 Förvaltningschef/RE-chef/avdelningschef

I enlighet med Danderyds kommuns styrdokument för informationssäkerhet ansvarar varje chef inom sitt ansvarsområde för att regelverket efterlevs.

I korthet omfattar personalansvariga chefers ansvar att:

- Anmäla nya medarbetare och medarbetare som slutat till ansvariga systemförvaltare
- Personalen är informerad om och efterlever kommunens regler för informationssäkerhet.
- Personal har rätt utbildning för att sköta sina uppgifter i systemet.
- Anlitad konsult och tredje part efterlever säkerhetsreglerna i dessa riktlinjer.
- Ge personalen möjlighet att delta vid säkerhetsutbildning.
- Avsätta tid för informationssäkerhet i lämpligt forum på arbetsplatsen.

Chefen har ansvar för alla informationstillgångar, och utrustning som är svår eller kostsam att ersätta. Chefen ska utfärda rutinbeskrivningar om hur informationen och utrustningen ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även märkta.

5.6 Medarbetare

Alla medarbetare och IT-användare inom Danderyds kommun ska följa det regelverk som finns kring informationssäkerhet inklusive de regler som finns för personligt ansvar vid systemanvändning. Alla ansvarar för att inhämta sådan information och att regelverket följs.
Vid oklarheter beträffande tillämpningen av detta regelverk ska varje anställd kontakta sin chef.

Oavsett om användandet sker privat eller i tjänsten ska gällande regler och lagar följas samt god moral och etik efterlevas. Endast de IT-verktyg som tillhandahålls via, eller i samråd med, IT-avdelningen samt är godkända av kommunledningen får

användas.

Medarbetare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks, samt se till att IT-utrustning inte utsätts för obehörigt användande av t.ex. familjemedlemmar. Pappersdokument och övriga lagringsmedia hanteras i enlighet med hur informationen har klassats.

5.7 Centrala specialistroller

5.7.1 Chefsarkivarien

Ansvarar för att informationen i kommunens system är åtkomlig för allmänheten enligt reglerna i offentlighets- och sekretesslagen 4 kap § 2 samt att den gallras och bevaras enligt besluten i myndigheternas dokumenthanteringsplaner.

5.7.2 IT-chef

IT-chefen har ansvaret för tillämpningen av Danderyds informationssäkerhet inom sitt ansvarsområde.

IT-chefen ansvarar för att:

- Rapportera avvikelser från styrdokument och riktlinjer till kommundirektören och informationssäkerhetschefen.
- Tillsätta resurser för IT-tekniska säkerhetslösningar inom ramen för den centrala IT-miljön

5.8 Roller i systemförvaltningsorganisation

5.8.1 Systemägare

I flertalet fall är systemägaren lika med den som är ytterst ansvarig för verksamheten och som ytterst ansvarar för informationen i systemet.

Inom informationssäkerhetsarbetet ansvarar systemägaren för att styrdokumentet för informationssäkerhet samt riktlinjer för informationssäkerhet efterlevs och att det finns en säkerhetsplan till systemet.

5.8.2 Systemförvaltare

Systemförvaltarens övergripande ansvar vad gäller informationssäkerhet är att ansvara för säkerhetsarbete avseende information (styrdokument för informationssäkerhet) samt ansvara för att nivån på systemsäkerhetsplanen upprätthålls.

5.8.3 Informationsägare

Informationsägaren har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägare fattar de avgörande besluten om information i systemen.

5.9 Ansvar personuppgifter

5.9.1 Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter i en verksamhet. I kommunen är respektive nämnd

personuppgiftsansvarig. Personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,
b) vad det skulle kosta att genomföra åtgärderna,
c) de särskilda risker som finns med behandlingen av personuppgifterna, och
d) hur pass känsliga de behandlade personuppgifterna är.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, skall den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

5.9.2 Kontaktombud personuppgifter

Kontaktombuden är de personer som utsetts av respektive nämnd att vara kontakten mellan personuppgiftsombud och respektive verksamhet. Kommunens respektive verksamheter ska anmäla sina personregister till kontaktombuden.

5.9.3 Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen, t.ex. en servicebyrå. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde. Personuppgiftsbiträdet ska genomföra de säkerhetsåtgärder som måste vidtas.

6 Samordning av informationssäkerhet

Säkerhetschefen har ansvaret för att utarbeta, förvalta och följa upp regelverket för informationssäkerheten. Efter förankring i kommunens förvaltningschefsgrupp godkänns och publiceras rutiner av säkerhetschefen.

7 Hantering av utomstående parter

Samverkan med konsulter, externa leverantörer och entreprenörer ska regleras genom avtal och alla ska ha kännedom om Danderyds kommuns regelverk kring informationssäkerhet samt följa detta.

8 Hantering av informationstillgångar

Tillgångar i detta sammanhang är det som för Danderyds kommun har ett värde i form av information (till exempel handlingar, dokumentation, datafiler, utbildningsmaterial, systemdokumentation), program (till exempel datorprogram, operativsystem, utvecklingsverktyg) och fysiska tillgångar (till exempel datorutrustning, telefoner, lagringsmedia).

8.1 Klassificering av information

Informationsklassning är en delprocess i den administrativa säkerheten i arbetet med informationssäkerhet.
Informationsklassning utgör grunden för hanteringen och behandlingen av information i kommunens informationssystem. För att komma fram till rätt skyddsnivå för information i informationssystem och databaser måste man veta vilken information som är viktig och varför den är viktig. Utifrån klassningen avgörs vem som har behörighet till informationen och hur informationen ska hanteras i olika situationer samt vilka delar av verksamheten som

är ömtåligast för störningar och dess konsekvenser.

Verksamhetsansvariga på samtliga nivåer i kommunen är ansvariga för att information som hanteras inom det egna verksamhetsområdet hanteras på ett korrekt sätt och ges ett adekvat skydd. Detta gäller oavsett om informationen hanteras elektroniskt eller manuellt. Informationsklassning ska genomföras vid all form av utveckling av nya och befintliga system. En informationsklassnings hållbarhet är kortvarig eftersom informationen fortlöpande förändras. Därför bör informationen klassas årligen eller oftare vid behov.

8.2 Märkning och hantering av information

Alla informationstillgångar, och utrustning som är svår eller kostsam att ersätta ska ha en utsedd ansvarig. Den ansvarige ska utfärda rutinbeskrivningar om hur informationen och utrustningen ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även märkta.

8.3 Arkivering och gallring

Den information som hanteras i kommunens informationssystem utgörs till stor del av allmänna handlingar. Av detta följer att denna skall bevaras, gallra och arkiveras som all annan information enligt bestämmelserna i lagar och myndigheternas dokumenthanteringsplaner.

9 Rekrytering, anställning och avslut av personal

Insatser för att minska riskerna för mänskliga misstag samt för stöld, bedrägeri och missbruk av informationstillgångar måste vara en viktig del av kommunens personalarbete.

9.1 Säkerhet vid rekrytering av anställd och inhyrd personal

Vid rekrytering bör kontroll och uppföljning av den arbetssökandes referenser och formella meriter, som CV, meritförteckning och yrkeslegitimationsinnehav, göras. En kontroll av den sökandes identitet bör också genomföras, för att klargöra att personen verkligen är den som den utger sig för att vara. Detsamma ska gälla vid anlitande av tillfällig personal. För vissa tjänster kan det komma att göras en framställan om registerkontroll enligt säkerhetsskyddslagen.

Vid anställningens **början** ansvarar varje användare för att:

- Ta del av den utbildning som ges i informationssäkerhet
- Ta del av samt följa det regelverk (informationssäkerhetspolicy, riktlinjer samt rutinbeskrivningar) som finns kring informationssäkerhet.

9.2 Säkerhet vid avslutande av anställning eller vid förflyttning

När medarbetare avslutar sin anställning eller byter arbetsenhet ansvarar varje chef för att behörigheter avslutas.

Vid anställningens **slut** ansvarar varje användare för att:

- Meddela vilka behörigheter som den anställda har haft så att de kan avbeställas av närmaste chef.
- Information som inte behövs för Danderyds kommuns framtida

verksamhet tas bort från servrar och datorer.

10 Fysisk säkerhet

Den fysiska säkerheten syftar till att skydda mot obehörigt tillträde och åtkomst, skador och störningar. Ett bra fysiskt skydd av lokaler, utrustning och dokument ska eftersträvas. Därför ska lokaler förses med passagekontroll, inbrottsskydd och brandskydd i den omfattning som krävs. En bedömning ska göras utifrån den verksamhet som bedrivs samt de krav som ställs utifrån lagar och förordningar. **Vid utformning av skyddsåtgärder måste det beaktas att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter.**

10.1 Riktlinjer för skydd av utrustning och information

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

För verksamheten kritisk IT-infrastruktur, IT-system och informationstillgångar ska inrymmas i säkra utrymmen, omgärdade av skalskydd, med lämpliga tillträdesspärrar och kontroller.

10.2 Tillträdeskontroll till byggnader och lokaler

Vid behov ska tillträdeskontroll till viktiga byggnader och lokaler finnas, för att säkerställa att endast behörig personal ges tillträde.

Inom kommunen ska det finnas rutiner så att det säkerställs att endast anställda och övriga behöriga personer vistas i lokalerna. Vilka som är behöriga att vistas i lokalerna avgörs av verksamhetsansvariga.

10.3 Säkerhet för utrustning utanför egna lokaler

Risker i samband med hantering av utrustning utanför de egna lokalerna ska beaktas. Detta gäller för informationsbärare i vid mening och omfattar bland annat persondatorer, handdatorer, mobiltelefoner och pappersdokument.
Rutiner/instruktioner skall fastställas för hur sådan utrustning skall hanteras. Dessa ska innehålla åtaganden från den anställde som kan komma att kvitteras. Viktigt är att även beakta riskerna då utrustning lämnas ut för extern service. Utförsel av utrustning och information ska vara godkänd av förvaltningschef.

10.4 Avveckling av utrustning

Lagringsmedia, som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning.

11 Styrning av kommunikation och drift

I dokumenten *Riktlinjer för IT* samt *Systemförvaltningsmodell* är hantering och krav på kommunikation och drift beskrivna.

11.1 Driftrutiner och ansvar

Målet är att säkerställa korrekt och säker drift av IT-miljön så att informationens sekretess, tillgänglighet, riktighet och spårbarhet bibehålls.

Ansvar och rutiner för incidenthantering skall vara etablerad. Mer information om detta finns i dessa riktlinjer för informationssäkerhet.

Driftansvar ska fördelas på olika personer för att minska risken för oavsiktlighet eller avsiktligt missbruk.

11.2 Kontroll av utomstående tjänsteleverantör

Utomstående leverantörer som bedriver verksamhet för Danderyds kommun kan för detta behöva tillgång till Danderyds nätverk. Informationssäkerheten och utförandet av tjänsterna ska ske enligt avtal och med bibehållen nivå av informationssäkerheten.

Det ska finnas en rutin för hur uppföljning och granskning ska göras på utomstående leverantörers tjänster.

I händelse av att rutinerna ändras eller att utförandet ändras på annat sätt ska en förnyad riskanalys göras. I händelse av att avtalet med tjänsteleverantören upphör ansvarar den som slutit avtalet att behörigheter till Danderyds nätverk avslutas och att informationstillgångar säkras.

11.3 Systemplanering och systemgodkännande

Alla informationssystem ska godkännas av systemägaren innan produktionssättning och vid förändringar i systemet ska en bedömning göras ifall godkännandet ska förnyas. En viktig parameter i ett godkännande är systemets klassning och dess skydd av informationen avseende sekretess, tillgänglighet, riktighet och spårbarhet.

11.4 Skadlig kod

Skadlig kod innehåller funktioner som har till syfte att påverka datorer, kommunikation och information på ett negativt sätt. Programvaror för skydd mot skadlig kod skall installeras av IT-avdelningen och kontinuerligt uppdateras på kommunens datorer.

11.5 Säkerhetskopiering

Den information som lagras på Danderyds kommuns gemensamma diskutrymmen säkerhetskopieras automatiskt. Information ska därför lagras på hemkatalog eller gemensamma kataloger enligt instruktioner från IT-avdelningen.

H: (personlig hemkatalog) är den personliga enheten som används för lagring av personligt arbetsmaterial och inte för allmänna handlingar. Om information lagras på denna enhet kommer andra medarbetare inte åt informationen men informationen säkerhetskopieras.

Informationen ska inte lagras på datorns hårddisk (C:). Undvik att lagra på hårddisken eftersom denna inte säkerhetskopieras och på grund av högre risk för att information kommer i orätta händer. Detta gäller både för stationära som för bärbara datorer.

När informationen ändå lagras på den lokala hårddisken (C:) är användaren personligen ansvarig för säkerhetskopiering. Den informationen som finns på den lokala hårddisken (C:) riskerar att förloras vid t.ex. en diskkrasch om den inte kan återskapas till rimliga kostnader. Information som är lagrad på en dators lokala hårddisk kan vid förlust av datorn bli tillgänglig för obehöriga. Om en bärbar dator som tillhör Danderyds kommun används måste användaren vara medveten om att datorn kan utgöra en säkerhetsrisk och att det därför inte får lagras sekretessbelagd eller för verksamheten hemlig information på den, om inte hårddisken har godkänd kryptering.

11.6 Styrning av nätverk

Skyddet av kommunens egna nätverk för informationsöverföring ska styras utifrån verksamhetens krav och kopplingar mot externa datanät. Hantering av säkerheten för nätverk, som kan sträcka sig över organisationsgränserna, kräver särskilda åtgärder.

11.7 Mediahantering och mediasäkerhet

Som flyttbara media räknas mobiltelefoner och läsplattor men också CD-/DVD-skivor, usb-enheter och externa hårddiskar. Dessa flyttbara media kan medföra stor skada om de innehåller sekretessbelagd information och kommer i orätta händer. Flyttbara media skall aldrig innehålla känslig information eller mer information än vad som är absolut nödvändigt. Vid undantag för detta ska kryptering av data användas.

11.8 Utbyte av information och program

Vid informationsutbyte mellan kommunen och andra organisationer eller externa parter ska gemensamma bedömningar göras av behovet av skydd mot åtkomst, skydd av riktighet samt kraven på tillgänglighet. Ansvarsförhållanden ska vara klarlagda. I kommunen ansvarar systemägaren för att ansvarsförhållandena är tydliggjorda.

Utbyte av information är t.ex. information som läses via dator, skickas med brev, e-post, skrivs på blädderblock eller whiteboard eller muntligt mellan människor både personligen och över telefon.

11.9 Elektroniskt offentliggjord information

Innan information görs allmänt tillgänglig på t.ex. webb-sida, ska åtgärder vidtas för att skydda riktigheten av informationen. Informationsägaren ansvarar för att information som publiceras av den egna verksamheten är korrekt, aktuell samt inte är sekretessbelagd.

11.10 Övervakning

Kritiska och säkerhetsrelevanta händelser i drift och datakommunikation ska vara spårbara.

Varje transaktion ska kunna knytas till den som utfört den. Detta ska i första hand åstadkommas med automatiska loggningsfunktioner. Behovet av loggning och uppföljning av loggar (analys) fastställs av systemägaren efter verksamhetens behov samt genomförd informationsklassificering.

12 Åtkomst till system och nätverk

12.1 Styrning av åtkomst till nätverk

Interna och externa nätverk är informationstillgångar och ska betraktas som sådana. Kommunens nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik.

Samtliga anställda i kommunen har åtkomst till kommunens nätverk. Det skall finnas tydliga rutiner för hur användarkonton och behörigheter hanteras i nätverket. Inte minst gäller detta avveckling av användarkonton och behörigheter vid byte eller avveckling av anställning. Det är närmaste chef som ansvarar för att en persons användarkonto och behörigheter är aktuella.

12.2 Styrning av åtkomst till operativsystem

Operativsystem och dess behörighetskontroll ska utformas så att möjligheterna till obehörig åtkomst minimeras.

12.3 Verksamhetskrav på styrning av åtkomst

Åtkomst till system och information ska styras utifrån verksamhetens behov och säkerhetskrav. Den som har behov av tillgång till viss information för att kunna utföra sina arbetsuppgifter ska tilldelas åtkomsträttigheter. All åtkomst ska vara baserad på behovsprincipen.

Systemägaren för respektive system beslutar om systemet och dess information ska vara tillgängligt från externa platser. Externa platser kan vara datorer utanför kommunens nätverk.

12.4 Styrning av användares åtkomst

Det skall finnas rutiner för att säkerställa de behörigas åtkomst och för att förhindra obehörigas åtkomst till kommunens information.

12.4.1 Styrning av åtkomst för administratörer

Alla administratörer ska ha individuella användaridentiteter. Användningen av verktyg eller hjälpmedel som gör det möjligt att kringgå eller åsidosätta säkerhetssystem och behörighetsskydd ska föregås av ett godkännande av IT-chefen. Inloggningsuppgifter som används för en specifik produkt vid leverans och andra standardlösenord med höga behörigheter ska förvaras skyddat.

13 Hantering av incidenter

13.1 Rapportering av säkerhetshändelser och svagheter

Incidenter och säkerhetsmässiga svagheter ska snarast rapporteras så att åtgärder kan påbörjas för att minimera skada, åtgärda brister och utreda eventuell brottslighet.

13.2 Hantering av säkerhetsincidenter och förbättringar

Om det finns misstanke eller det upptäcks att en användare i Danderyds kommuns nät har använt en dator till något olagligt eller till något som bryter mot kommunens styrande dokument ska detta anmälas till användarens chef.

Om det upptäcks fel och brister i de system som används ska detta rapporteras till systemägaren och vid allvarligare fel och brister till IT-chef. IT-avdelningen bedriver genom övervakning av nätverk, logganalys och stickprover ett förebyggande arbete för att förhindra uppkomsten av incidenter.

14 Förvaltning av detta dokument

Informationssäkerhetschefen ansvarar för dessa riktlinjer. Kommundirektören fastställer riktlinjerna. Uppdatering skall ske vid behov. Riktlinjerna skall ses över minst vart tredje år.

15 Efterlevnad

En väl fungerande informationshantering bidrar till att kommunen kan fullgöra sina uppgifter. Det är därför viktigt att lagar och förordningar följs.

15.1 Efterlevnad av rättsliga krav

Områden som är av särskild vikt att beakta efterlevanden av är t.ex.:

- Arkivlagen
- Arkivförordningen och gallringsförordningen
- Personuppgiftslagen
- Offentlighet och sekretesslagstiftning
- Upphovsrättslagen
- Bokföringslagen och –förordningen
- Lagen om kommunal redovisning
- Särskild myndighetslagstiftning

15.2 Efterlevnad av riktlinjer för informationssäkerhet

Vid överträdelse av Riktlinjer för informationssäkerhet kommer detta anmälas till kommundirektören och ärendet kommer att behandlas i enlighet med kommunens personalpolicy.

Du är som användare personligen ansvarig för dina handlingar. Alla olagliga aktiviteter med kommunens informationshantering kommer att polisanmälas och utredas.

15.3 Arbetsgivarens rättigheter

Revisioner av användandet av informationssystem kan genomföras löpande inom Danderyds kommuns alla informationssystem och IT-miljö. Detta omfattar hela kommunens verksamhet.

All information, informationsbehandlingsresurser samt kringutrustning och konton

ägs av Danderyds kommun. Detta innebär att allt som finns på datorerna, i nätverk och i molnet samt i arkiv är Danderyds kommuns egendom. Arbetsgivaren har rätt att kontrollera transaktioner som medarbetare har utfört i kommunens nätverk, vad som finns i datorn, telefonen, e-post och hemkataloger som medarbetarna använder, samt att återställa infrastruktur och data i enlighet med detta regelverk. Se även under punkt 11.10.

I varje enskilt fall där någon verksamhet begär att göra avsteg från detta regelverk eller de övriga dokument som beskriver riktlinjer och rutiner avseende informationssäkerhet ska detta godkännas av informationssäkerhetschef i samråd med kommundirektör.
Grund för begäran för avsteg kan vara stöd för att utveckla verksamheten och där det befintliga regelverket sätter hinder.

Undantag ska dokumenteras och bör normalt vara tidsbegränsande.

16 Ordlista

Informationssäkerhet
Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad sekretess, riktighet, tillgänglighet och spårbarhet. Begreppet innefattar både fysisk säkerhet, IT-säkerhet samt administrativ säkerhet.

Informationsteknik
Den teknik som används för att på elektronisk väg samla in, lagra, bearbeta, kommunicera samt presentera data, bild, text och ljud. Den omfattar all användning av elektronisk informationsteknik och omfattar därmed samtliga skolsystem, vård och omsorgssystem, geografiska informationssystem, administrativa stödsystem, allmänna informationssystem samt system som är eller kan kopplas upp på nätverk. Datorer med kringutrustning, nätverk, tekniska stödsystem (operativsystem, databas, säkerhet, virusskydd, med mera), telefonkommunikationslösningar omfattas också.

Informationstillgångar
En organisations skyddsvärda informationsrelaterade tillgångar. Exempel på informationstillgångar är:

- Information (databaser, filer, metodik, dokument, etc.)
- Program (tillämpningar, operativsystem, etc.)
- Tjänster (nätförbindelser, abonnemang, etc.)
- Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)

Incident
En händelse som avviker från det normala och som innebär en störning eller överhängande risk för störning i det dagliga arbetet, potentiellt kunde händelsen ha orsakat allvarliga konsekvenser för verksamheten.

Kontinuitetsplan
Dokument som beskriver hur verksamheten ska bedrivas och återställas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.

Personuppgift
All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Personregister
Digitala eller manuella register som innehåller personuppgifter.

Rutinbeskrivning
Dokument som beskriver som detaljerat redogör för hur rutiner och säkerhetslösningar ska utformas och tillämpas, för att Informationssäkerhetspolicyns krav ska efterlevas.

Andra namn på en rutinbeskrivning kan vara instruktion, anvisning eller rutin.

Tillgång
Allt som är av värde för Danderyds kommun. Innefattas förutom informationstillgångar även immateriella värden, som t.ex. goodwill.

26 februari 2013

Johan Haesert
Kommundirektör