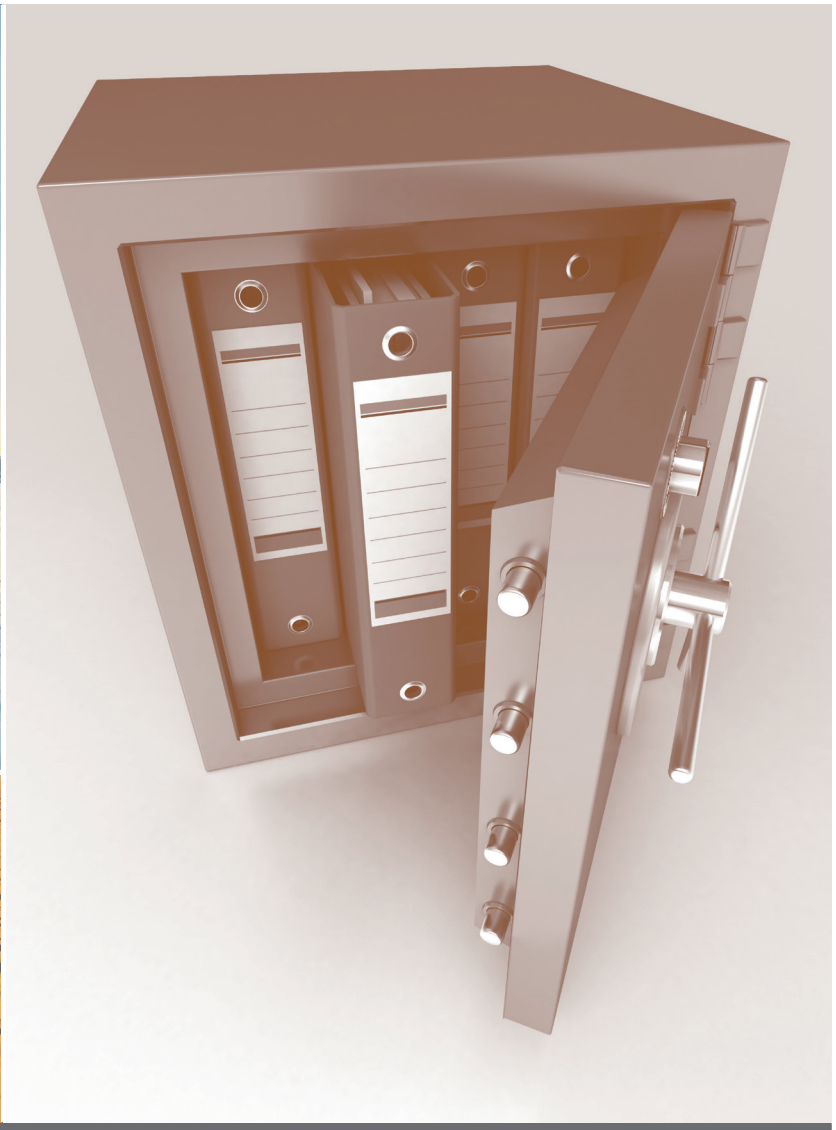
LULEÅ KOMMUN

• • • Riktlinjer



Informationssäkerhet för användare

RIKTLINJER

INFORMATIONSSÄKERHET

FÖR ANVÄNDARE

inom Luleå kommunkoncern

Dokumenttyp	Dokumentnamn	Beslut antaget/fastställt
Riktlinje	Informationssäkerhet för användare inom Luleå kommunkoncern	Kommundirektör 2015-10-01
Version	Dokumentansvarig	Reviderat
1.4	KLF IT-chef	

Förord

En god informationssäkerhet är idag en absolut nödvändighet för alla organisationer. Hoten mot våra informationstillgångar är många och ökar ständigt. Luleå kommunkoncerns alla verksamheter är beroende av att informationen är tillgänglig för rätt person vid rätt tidpunkt och att den är riktig för att kunna fullfölja sina uppdrag och ge god service till medborgare och andra intressenter. Därför måste vi i likhet med andra organisationer säkerställa att informationen är skyddad och att ställda informations-säkerhetskrav är uppfyllda. Samtliga anställda i Luleå kommunkoncern har ett eget ansvar för att upprätthålla en god informationssäkerhet.

Anne Karlenius, Kommundirektör

1 INLEDNING

Kommunens alla verksamheter är beroende av att dess information är tillgänglig för rätt person vid rätt tidpunkt samt att den är riktig och därmed kan utgöra ett bra beslutsunderlag.

Hoten mot våra informationstillgångar är många, och för att säkerställa att informationen är skyddad finns vissa informationssäkerhetskrav som måste uppfyllas. Samtliga anställda i Luleå kommunkoncern har ett ansvar för att säkerställa god informationssäkerhet.

Du som är medarbetare och därmed användare av kommunens information ska känna till:

- vilka krav som ställs på dig inom informationssäkerhet
- vad du ska göra vid incidenter (exempelvis att informationen inte är tillgänglig, du misstänker virusangrepp eller dataintrång, information har ändrats eller förstörts, stöld eller förlust av datautrustning)
- att du kan få stöd och hjälp från din chef, systemägaren, systemförvaltaren, systemadministratören eller IT-support

Ramarna för Luleå kommunkoncerns informationssäkerhetsarbete baseras på gällande lagar samt för Luleå kommun anpassade föreskrifter. Dessa reglerar hanteringen av kommunens informationstillgångar, däribland skyddet av personlig integritet.

Alla som är i kontakt med kommunens information och utrustning har ett ansvar att skydda densamma. Policyn med tillhörande riktlinjer ska, av chef eller motsvarande, kommuniceras med samtliga medarbetare på lämpligt sätt.

2 STYRANDE DOKUMENT FÖR INFORMATIONSSÄKERHET

- Informationssäkerhetspolicy

- Riktlinjer - informationssäkerhet för användare inom Luleå kommunkoncern (detta dokument)
- Riktlinjer - informationssäkerhet för systemägare & systemförvaltare (under bearbetning)
- Säkerhetsanvisningar för mobila enheter (bilaga till Riktlinjer - informationssäkerhet för användare inom Luleå kommunkoncern)
- Riktlinjer för roller och ansvar inom informationssäkerhet och systemförvaltning
- Ärendehantering i Luleå kommun

Utöver dessa dokument så har kommunen utarbetat IT-policy och IT-strategi samt att enskilda verksamhetssystem har egna tillämpningsanvisningar. Om efterlevnaden är god även av innehållet i dessa dokument så bidrar detta till kommunens systematiska arbete för att skydda informationen mot hot och därmed bevara förtroendet för den kommunala verksamheten.

Informationssäkerhet är en del av kommunens interna säkerhetsarbete. Kommunens agerande och organisation vid extraordinära händelser, agerande vid personliga hot, riskbedömningar för skador och störningar på kommunens verksamhet, systematiskt brandskyddsarbete, försäkringsfrågor, personlig säkerhet etc finns beskrivna i andra styrande dokument.

”Riktlinjer - informationssäkerhet för användare” ska tillämpas inom Luleå kommunkoncern, med undantag för krav som respektive bolags ledning bedömer står i konflikt med Luleå kommunföretags ägardirektiv och är beslutad enligt egen riktlinje.

3 VAD ÄR INFORMATIONSSÄKERHET

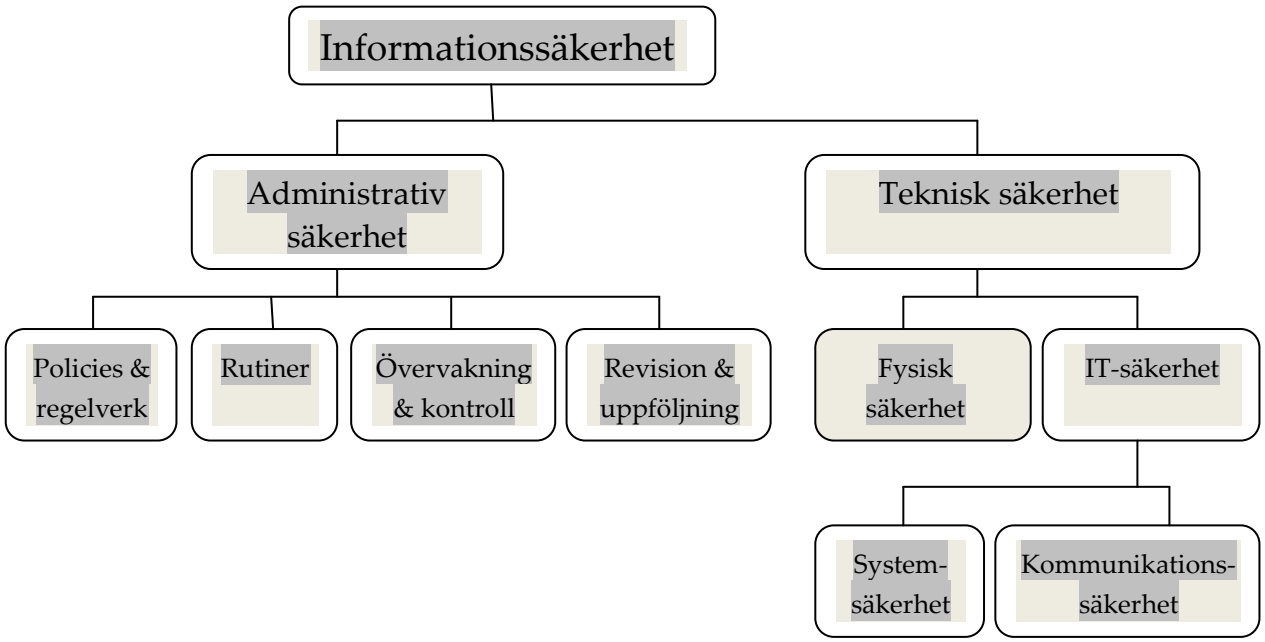
Information kan vara talad, skriven eller tryckt på papper, elektronisk/digital och som digital förpackad i bild-, film eller ljudformat. Exempel på information i kommunen är föreskrifter om vad som gäller för en kommunal tjänst för medborgarna, politisk handläggning och beslut, tjänstemannabeslut eller rådgivning, uppgifter om anställd personal, omvårdnadsdokumentation, dokumentation om elever, betyg, förbrukning av vatten och el, kartmaterial, m m.

Med informationssäkerhet avses skydd av informationstillgångar med syftet att upprätthålla nödvändig nivå avseende:

- Tillgänglighet; att informationstillgångar är tillgängliga för behörig användare i avsedd utsträckning
- Riktighet; att informationstillgångar inte förändras eller förstörs av misstag eller av obehörig
- Konfidentialitet; att informationstillgångar inte avslöjas eller blir tillgängliga för obehörig
- Spårbarhet; möjlighet att entydigt kunna härleda utförda aktiviteter i systemen till en identifierad användare

Behovet av skyddsåtgärder utifrån begreppen tillgänglighet, riktighet, konfidentialitet och spårbarhet är olika beroende på hur verksamheten har klassat informationen. Informationsklassningen har stor betydelse för hur du förväntas agera.

Informationssäkerhetens omfattning beskrivs ofta enligt nedanstående figur.



4 INFORMATIONSSÄKERHETSRÅD OCH ETISKT RÅD

4.1 Informationssäkerhetsråd

Kommunen avser att inrätta ett informationssäkerhetsråd med deltagare från förvaltningar och bolag. Förutom informationssäkerhetssamordnare, kommunarkivarie och kommunjurist deltar antingen verksamheternas IT-samordnare eller personuppgiftsombud.

Rådets uppgifter är att genom erfarenhets- och kunskapsutbyte utveckla kommunens arbete med informationssäkerhet på en övergripande nivå, men också bevaka vilka behov av stöd som verksamheterna behöver och föreslå förbättringar. Rådet ska dessutom bevaka efterlevnaden av att kommunen arbetar på ett informationssäkert sätt i enlighet med kommunens styrdokument och lagstiftning. Rapportering och förslag till beslut läggs till kommundirektörens ledningsgrupp.

Delar av rådet (IT-chef, IT-controllerchef, informationssäkerhetssamordnare samt kommunjurist) utgör beslutande grupp för att ta ställning till rapporterade informationssäkerhetsincidenter med mandat att agera omedelbart och genomföra åtgärder. Beroende på incidentens karaktär kan berörd förvaltningschef, bolagschef, säkerhetschef eller kommundirektör kallas in för att medverka vid bedömning och beslut om åtgärd. Rapportering av genomförda åtgärder görs till kommundirektörens ledningsgrupp.

4.2 Etiskt råd för blockering av hemsidor

Kommunen vill markera att den arbetar aktivt mot kränkande beteende på nätet och inte tillåter åtkomst av en hemsida som etiska rådet beslutat att blockera från kommunens nätverk. Blockering av hemsida innebär dock inte att kommunen förhindrar åtkomst från mobiltelefoner eller från andra nätverk.

En begäran om blockering kan ställas till IT-kontoret som sammankallar det etiska rådet. Det etiska rådet har representanter från Socialförvaltningen, Barn- och utbildningsförvaltningen, Kommunikationskontoret, Personalkontoret samt från IT-kontoret.

Rådets beslut kommuniceras till den/de som initierat begäran. Om en begäran om blockering bifalls så kommunicerar Kommunikationskontoret detta på lämpligt sätt.

5 ÅTKOMST TILL INFORMATIONEN

5.1 KLASSNING

Verksamhets- och samhällsviktig information i Luleå kommun klassas av systemägare och systemförvaltare utifrån aspekterna tillgänglighet, riktighet, konfidentialitet och spårbarhet (definitioner, se avsnitt 3).

Det är klassningen som avgör hur informationen ska skyddas. Då du som användare ska flytta eller spara information till annat media (exempelvis extern hårddisk, USB-sticka eller annan nätverksplats) behöver du känna till hur den är klassad för att kunna avgöra var och hur du får lagra den. Information kan vara klassad i tre olika nivåer;

- Grundsäkerhetsnivå (exempelvis information som kommunen kan publicera som öppna data eller att konsekvenserna är lindriga om informationen är otillgänglig ett par dagar)
- Mellan (t ex ekonomisystem)
- Hög (t ex socialtjänstens verksamhetssystem)

Klassningen lägger betydande vikt vid att offentlighetsprincipen gäller oavsett informationsbärare. Information som lagras elektroniskt ska ha samma tillgänglighet som information lagrad på annat sätt.

5.2 BEHÖRIGHET OCH INLOGGNING

Chef, eller av denne utsedd person, registrerar anställningsuppgifter i kommunens Personalsystem. När din anställning i kommunen träder i kraft erhåller du behörighet till kommunens nätverk, hemmakatalog (H:), intranätet, Internet, Word/Excel/Powerpoint, utskrifter, generella IT-system samt e-post.

I samband med din första inloggning i Luleå kommuns nätverk får du ett välkomstbrev via e-posten där du uppmanas att gå igenom en självstudiekurs i grundläggande IT-säkerhet, Datorstödd Informationssäkerhetsutbildning för Användare (DISA), främst inriktad mot vad du som användare bör tänka på. Nyanställda i bolagen LLT, LRAB, Luleå Hamn AB och Kronan erhåller samma uppmaning i brev från respektive IT-samordnare.

Första gången som du loggar in med det tilldelade lösenordet i nätverket byter du omedelbart lösenord till ett lösenord som bara du känner till. Det är vanligt att den principen används som första åtgärd för nya IT-system som du får behörighet till, nämligen att du får ett preliminärt lösenord som du vid första inloggningen omedelbart ska byta.

Om du har glömt lösenordet till nätverket så finns en instruktion på intranätet som beskriver hur du med hjälp av medarbetare på plats själv åtgärdar problemet. Ifall du väljer att kontakta IT-support så tillämpas motringning. Ett nytt tillfälligt lösenord lämnas enbart ut på ett telefonnummer som finns i kommunens förteckning.

Systemförvaltare för respektive system ansvarar för att ge dig behörighet till de verksamhetsspecifika system som du använder i arbetet. Användarnamn och lösenord distribueras till dig antingen via din chef eller från din systemförvaltare per epost.

5.3 BEHÖRIGHET FÖR EXTERNA ANVÄNDARE

Externa användare, exempelvis konsulter, behöver ibland behörighet till nätverk och system. Systemförvaltaren eller systemägaren ska i sådana fall göra en ansökan om behörighet för konsulten, som personligen skriver under både behörighetsansökan samt sekretessförbindelse. Konsulten ska inte ha tillgång till mer information än denne behöver för sitt uppdrag.

Externt anlitad eller inhyrd personal får endast ansluta medhavd dator eller annan utrustning till kommunens trådlösa gästnät (LK_GUEST). För dessa är det inte tillåtet att ansluta till kommunens administrativa nät (LK_NET) eller till kommunens resursnät.

Detaljer om rutiner för externa användares åtkomst hittar du i dokumentet "Fjärråtkomst till Luleå kommuns verksamhetssystem, servrar och nät", daterat 2014-03-20.

5.4 LÖSENORD

Lösenordet som är kopplat till ditt användarnamn, är till för att förhindra obehöriga från att få tillgång till kommunens information.

Vissa system/applikationer har regler för hur lösenordet ska vara konstruerat, andra tillåter ”enklare” lösenord. Tänk dock på att om du väljer ett enkelt lösenord underlättar du för eventuella angripare att ta sig in i kommunens nätverk och system.

Tänk på detta då du väljer lösenord:

- lösenord är personliga och det är ditt ansvar att se till att ingen annan känner till dina lösenord
- när du dokumenterar lösenord så ska det vara på ett säkert sätt
- lösenordet ska vara minst 6 tecken långt.
- använd inga riktiga ord som lösenord
- använd inte heller namn på familjemedlemmar, husdjur, telefonnummer el dylikt som kan kopplas till dig personligen.
- lösenordet bör bestå av stora och små bokstäver samt siffror och specialtecken - i de fall applikationen/systemet tillåter det
- du får inte använda samma lösenord i kommunens system som de du använder hemma
- återanvänd inte lösenorden
- byt lösenord på nätverket och för eposten när du uppmanas göra detta (8 ggr per år) samt minst 4 gånger per år i verksamhetssystem som inte har fastställt bytesintervall.

6 DIN ARBETSPLATS

6.1 UTRUSTNING FÖR DIG SOM ANSTÄLLD AV KOMMUNEN

IT-kontoret har ansvaret för kommunens nät. Det innebär att endast personal från IT-kontoret, eller av IT-kontoret anvisad personal från underleverantör, har rättighet och behörighet att ansluta utrustning till nätet, göra kopplingar/omkopplingar i det fysiska datanätet och liknande insatser.

Det innebär också att endast av IT-kontoret godkända och anvisade fabrikat & modeller får beställas och användas.

För din dator med tillhörande utrustning gäller dessutom följande:

- om du behöver ytterligare utrustning för att kunna klara av dina arbetsuppgifter ska du anmäla detta till din chef som i sin tur beställer den utrustning som behövs

- fel ska omedelbart anmälas till IT-support
- ingen anslutning av privat utrustning till kommunens nätverk tillåts, förutom till det publika gästnätet LK_GUEST

6.2 ANSLUTNING FÖR ELEV, MEDBORGARE & EXTERN

Kommunens skolelever ansluter till Internet via trådlös uppkoppling. De s k skoldatorerna får inte anslutas till det fasta nätverket (via fasta uttag).

Kommunen tillhandahåller publik trådlös Internetåtkomst på flera platser, t ex i Kulturens Hus, på skolor, i stadshuset och på flertalet arbetsplatser. Där är det tillåtet att ansluta privata dataenheter till det publika nätet LK_GUEST. Åtkomst till Internet tilldelas med koppling till användaren, med tidsbegränsning och med begränsning av trafikmängd. Trafiken på Internet loggas och sparas (spårbarhet) för att användas vid eventuell utredning om missbruk.

6.3 PROGRAM OCH APPLIKATIONER

Arbetsgivaren tillhandahåller program och applikationer som du behöver i ditt arbete.

För bärbar eller stationär arbetsplatsdator finns kraftiga begränsningar för vad du själv kan ladda ned. Vid nedladdning av möjliga valbara applikationer, är rådet att vara försiktig och att du hellre frågar om råd en gång för mycket i stället för inte alls.

Kommunen har tills vidare lagt få begränsningar för nedladdning av applikationer till läsplattor och smarta mobiler. Rådet är därför att vara extra försiktig innan du bestämmer dig för att ladda ned en applikation till dessa dataenheter.

Övriga saker som du ska känna till:

- det är inte tillåtet att kopiera eller använda kommunens program utanför kommunens verksamhet
- det är inte tillåtet att använda kommunens program för mer än det du behöver i ditt arbete, exempelvis att söka information i verksamhetssystem för privata ändamål. Det ska finnas en relation till dina arbetsuppgifter, i annat fall finns risk för dataintrång
- vissa verksamhetssystem lyder under hälso- och sjukvårdslagstiftning och är därmed belagda med striktare regler som bland annat påbjuder regelbundna åtkomstkontroller av användarna

- använd inte någon annans inloggning; de enda undantagen från detta gäller för självklara händelser såsom akut situation med fara för hälsa, liv eller skada på egendom

Vidare så är det enligt lag förbjudet att:

- sprida information via Internet eller därmed sammankopplade nätverk som bryter mot svensk lagstiftning, som t.ex. barnpornografi, förtal eller yttranden som kan ses som hets mot folkgrupp
- utföra marknadsföring genom massutskick av e-post (spam) eller s k mailbombning om mottagaren ej i förväg gett sitt samtycke till detta
- utnyttja någon annans identitet eller IP-adress, eller försöka att göra det
- ladda hem, lagra eller sprida dataprogram, musik, bilder och filmer eller annat copyrightskyddat material utan tillstånd av upphovsmannen

6.4 NÄR DU LÄMNAR DIN ARBETSPLATS

- stäng alltid av datorn när du går hem för dagen och logga ut från nätverket om du lämnar arbetsplatsen för en längre stund, kravet avser både säkerhet och ur energisynpunkt
- när du lämnar datorn utan uppsikt, lås datorn tillfälligt antingen med tangenterna Ctrl+Alt+Delete och välj Lås Arbetsstation eller använd tangenterna windowsflaggan+L
- lås in personakter och annat sekretessbelagt material enligt instruktioner på din arbetsplats
- om möjlighet finns och din chef kräver det så lås dörren när du avslutar för dagen eller lämnar rummet

6.5 SERVICE OCH KASSERING

IT-kontoret köper in datorer och tillhandahåller datorarbetsplats som tjänst för kommunens verksamheter. Datorerna byts ut till nya efter ca tre års användning.

- när du byter ut/lämnar tillbaka din dator, kontrollera att det inte finns lagrat information på hårddisken C:\. Flytta i så fall den informationen och radera den därefter från hårddiskens C:\

- all installation och service av din dator utförs av IT-kontoret eller av denne anlitad underleverantör

7 DISTANSARBETE

7.1 ARBETE HEMIFRÅN ELLER ANNAN PLATS

När du jobbar utanför kontoret är det extra viktigt att tänka på säkerheten. Jobbar du hemifrån bör du särskilt tänka på att:

- du ansvarar för din dator (och annan kommunägd utrustning) när du tar med den utanför kommunens lokaler. Det innebär att du ska skydda den från stöld och åverkan genom att förvara den på ett säkert sätt och inte lämna den obevakad i bilen om du stannar för att uträtta ärenden
- inte lagra arbetsrelaterad information på en privat dator
- inte lämna datorn obevakad så att exempelvis familjemedlemmar kan se ditt arbetsmaterial
- inte låta exempelvis familjemedlemmar använda din jobbdator eller annan kommunägd utrustning
- inte använda privat e-post till arbetsrelaterad information
- kommunens klientplattform medger åtkomst av information oavsett var du befinner dig, förutsatt internetåtkomst. Undvik därför användning av USB-sticka för överföring eller lagring av information
- om du ansvarar för extern föreläsare och denne vill använda information från egen medhavd USB-sticka så bör du försäkra dig om att föreläsarens USB-sticka är krypterad enligt kommunens anvisningar.

Jobbar du på annat ställe utanför kontoret, exempelvis på tåg, så tillkommer att du bör tänka på:

- Använd ett insynsskydd på datorskärmen om du jobbar med känslig information. Skyddet förhindrar att någon obehörig kan läsa information från din skärm, såvida personen inte sitter mitt framför skärmen.
- Om du talar i telefonen, tänk på att du inte vet vem som kan lyssna. Prata därför inte om saker som kan vara känsligt om du inte har försäkrat dig om att ingen annan kan avlyssna samtalet

Övrigt gällande distansarbete, se riktlinjen "Distansarbete" (2010-12-15)

7.2 ANVÄNDNING AV MOBILA ENHETER

Se bilagan till denna riktlinje, "Säkerhetsanvisningar för mobila enheter", bilagan beskriver saker att tänka på om du använder mobiltelefon och/eller läsplatta. Säkerhetsanvisningarna finns också med som bilaga längst bak i detta dokument.

8 LAGRING

All information som finns i verksamhetssystemen är Luleå kommuns egendom och lagras på gemensamma resurser. Information som lagras på de gemensamma resurserna säkerhetskopieras och förvaras på säkert ställe.

Det finns mycket mer som produceras av dig som anställd i kommunen och som inte placeras direkt i verksamhetssystem. Fortsatt gäller att tjänstedokument ägs av Luleå kommun men att det finns flera olika ställen att lagra informationen på. Var du bör lagra din information beror på vilken typ av information det handlar om. Vissa lagringsytor är mer känsliga än andra. Klassificering av informationen avgör var den ska, eller inte ska, lagras.

Kommunen arbetar med införandet av ett dokumenthanteringssystem som, när det är infört, lagrar merparten av de dokument som produceras i kommunen oavsett om dokumenten är att betrakta som allmän handling eller arbetsmaterial. Systemet innebär bl a att du som användare inte behöver fundera på var dokument lagras, systemet sköter detta åt dig på ett korrekt, organiserat och lättillgängligt sätt sedan du angett metadata för dokumentet.

Fram till dess att dokumenthanteringen är automatiserad så gäller nedanstående stycken och tabellen:

Din personliga hemmakatalog H: bör endast användas för att lagra arbetsrelaterat material av känslig karaktär och material som du själv använder dig av i arbetet. Tänk på att ingen annan än du själv har åtkomst till H:. Det kan innebära att tillgängligheten till viktiga dokument försvåras för dina medarbetare under din frånvaro. Lagra därför merparten arbetsrelaterat material på V:.

Lagringsytan C: innebär lokal lagring på din dator och data på C: säkerhetskopieras inte. C: kan endast användas för personliga syften, helt och hållet under eget ansvar.

Lagringsyta	**Säkerhetsbedömning**	**Säkerhetskopiering**	**Lämpligt för vilken typ av information?**
V – förvaltningens lagring av information	Kommunens lagringsyta. Skyddad från obehörig åtkomst.	All information säkerhetskopieras	Förvaltningens gemensamma information som delas av alla eller att den enbart är synlig för exempelvis en arbetsgrupp
H – din personliga hemmakatalog	Kommunens lagringsyta. Skyddad från obehörig åtkomst.	All information säkerhetskopieras	Endast du har tillgång till informationen på H. Mtrl av känslig karaktär & eget bruk.
C - Lokalt på din dator	Spara på C innebär risker, ingen säkerhetskopiering, endast skyddad av inloggning till datorn.	Ingen säkerhetskopiering	Här ska ingenting sparas som har något med arbetet att göra.
Arbetsrum (dokument-hantering i Sharepoint och på intranätet)	Kommunens lagringsyta. Skyddad från obehörig åtkomst	All information säkerhetskopieras	Används av projekt och arbetsgrupper med behov av att dela dokument. När arbete avslutas placeras dokumenten på V:
Intranätet	Kommunens lagringsyta. Skyddad från obehörig åtkomst	All information säkerhetskopieras	All dokumentation som arbetsledning beslutat ska vara tillgängligt på intranätet placeras också där, oftast med kopia på annan plats
Outlook – kommunens epostsystem	Kommunens lagringsyta. Skyddad mot obehörig åtkomst	All information säkerhetskopieras	Endast du har tillgång till informationen. Begränsat utrymme – spara helst bifogade filer i epost på H: eller V: . Bedöm om mottagen epost ska diarieföras eller inte – radera allteftersom

Mobiltelefon, smart phone, läsplatta	Osäker lagring. Dåligt skyddad. Något bättre om pinkod används (pinkod används om mobilen synkroniseras med epost)	Ingen säkerhetskopiering	Här ska du inte lagra någonting
USB-sticka, extern hårddisk	Osäker lagringsyta, dock innebär en krypterad sticka att det blir omöjligt att läsa från en stulen enhet	Ingen säkerhetskopiering	Undvik användning av USB-sticka eller hårddisk i arbetet för temporär lagring och överföring av data. Uteslutet att lagra integritetskänsliga dokument om enheten är okrypterad
Extern lagring i moln (Dropbox, Google etc)	Extern leverantör av lagringsyta. Kommunen har ingen kontroll på detta. Skyddat mot obehörig åtkomst, oftast försedd med krypterad trafik.	Ingen säkerhetskopiering hos kommunen. De större leverantörerna har troligtvis säkerhetskopiering.	Här sparas ingen information som innehåller persondata, känsligt och/eller sekretessbelagt material. Om molntjänst används får den endast innehålla dokument av publik karaktär

9 INTERNET

All Internetsurfning i kommunens nät loggas vilket betyder att det finns möjlighet att se vilka sidor som besökts och av vem. För att titta på loggar krävs förekommen anledning samt beslut av verksamhetschef/kontorschef eller motsvarande. Loggar sparas en månad och raderas automatiskt.

- Du som använder Internet har ett personligt ansvar för att följa kommunens etiska regler som de kommer till uttryck i detta dokument och det som kommunens etiska råd beslutar om fortlöpande
- Du som använder Internet är ansvarig för allt som görs med din användaridentitet och naturligtvis att följa svensk lag
- Det är inte tillåtet att ladda ned filer till din dator för privat bruk

- Eftersom kommunens användaradress alltid framgår när vi är uppkopplade, är det viktigt att tänka på att vi representerar kommunen i varje kommunikation på Internet. När du surfar så registreras ofta kommunens adress och de sidor du besöker av Internetsitens ägare
- Det är inte tillåtet att ladda hem, lagra eller sprida dataprogram, musik, bilder och filmer eller annat copyrightskyddat material utan tillstånd av upphovsmannen.

Om ditt arbete innebär att du publicerar information på intranätet eller på den externa webbplatsen lulea.se så ska du känna till innehållet i "Riktlinjer för Luleå kommuns intranät och externa webbplats lulea.se" (2012-12-07).

9.1 REPRESENTERA KOMMUNEN I SOCIALA MEDIER

Användandet av sociala medier, såsom Facebook, Twitter, flickr och andra bloggar har ökat den senaste tiden. Det finns säkerhetsrisker även med användandet av dessa applikationer. För din egen och arbetsgivarens skull finns det saker du bör tänka på när du skapar och använder ditt konto.

Ta del av och följ kommunens riktlinjer om du får uppdraget att skapa ett konto i ett socialt forum.

Detaljerade instruktioner för kommunens användning av sociala medier återfinns i dokumentet "Riktlinjer för sociala medier" (2011-12-06)

9.2 PRIVATA KONTON I SOCIALA MEDIER

Kommunen ansvarar inte för konton/sidor som anställda skapat och där den anställde representerar sig själv som privatperson. Den anställde ska däremot även i dessa forum respektera sekretessen gentemot arbetsgivaren, kollegor och brukare, genom att inte publicera personuppgifter eller känslig information kring dessa.

Om du gör inlägg som handlar om personer du kommer i kontakt med via ditt jobb, tänk då på att man med ganska lite information kan gissa sig till vem personen ifråga är, och att du därmed riskerar, särskilt om inläggen uttrycker negativa omdömen, att inlägget klassas som felaktig hantering av personuppgifter.

10 E-POST

Några saker av särskild säkerhetsmässig vikt vid användning av e-post:

- Det är inte tillåtet att skicka integritetskänslig eller sekretessbelagd information via e-post
- Det är inte tillåtet att vidarebefordra din e-post i arbetet till din privata e-postadress
- Kontrollera alltid mottagaren en extra gång, särskilt om du svarar på ett brev, så att du inte av misstag skickar e-posten till fler/andra mottagare än du avsett.
- Använd inte din kommunala epostadress i privata sammanhang, såsom användarnamn på sociala forum eller då du anmäler dig till tävlingar på internet.
- Använd inte din privata epostadress till att skicka arbetsrelaterad e-post
- Förvissa dig om vilka regler som gäller på din arbetsplats för vidaresändning till kollega om du på grund av ex v sjukdom, semester, tjänstledighet för studier eller annat arbete inte öppnar e-posten på en vecka eller längre
- Om du vid distansarbete behöver åtkomst till arbetsrelaterad e-post, så är det mer säkert att öppna din kommunala brevlåda på webben jämfört med att vidaresända arbetsrelaterad e-post till privat brevlåda. Självklart med beaktande av normal försiktighet som gäller för allt distansarbete.

En mer uttömmande beskrivning av saker att tänka på för e-post återfinns i dokumentet "Ärendehantering i Luleå kommun" (2013-01-21).

11 INCIDENTER, VIRUS, "FISKE" EFTER ANVÄNDARKONTO/BANKKONTO

11.1 INFORMATIONSSÄKERHETSINCIDENTER

Incident är en plötslig och oönskad händelse som redan har gett eller kan komma att ge negativa konsekvenser för verksamheten eller en enskild individ. Ett exempel på incident är ett stopp i nätverket som innebär att ingen kommer åt information eller kan skriva i journaler, ett annat exempel är att nätverket fungerar men ett enskilt verksamhetssystem inte är tillgängligt eller fungerar dåligt, ett tredje exempel är att du påträffar data som är uppenbart oriktiga och ett fjärde att personer som inte borde ha åtkomst till viss information uppenbarligen har det i alla fall.

Ovetskap om en Internetadress eller ett borttappat lösenord är inte incidenter utan löses snabbt på annat sätt med berörda.

Om du upptäcker att nätverket inte fungerar eller att ett verksamhetssystem inte är tillgängligt så kontaktar du IT-support för felrapport och åtgärd. Beroende på problemets omfattning och orsak så bedömer IT-support om det ska rapporteras som incident eller inte. I det första fallet gör IT-support en incidentrapport.

Om du upptäcker fel och brister i de system du använder är det oftast inte en informationssäkerhetsincident, utan detta rapporteras till systemförvaltare, systemadministratör eller närmaste chef.

Om du uppmärksammar att personer som inte borde ha åtkomst till information uppenbarligen har det, så fyller du i det formulär som finns på intranätet som heter ”Rapport informationssäkerhetsincident” och sänder iväg rapporten efter ifyllnad. Incidentrapporten hamnar som inkommet ärende hos IT-supporten, besvaras (och åtgärdas) antingen direkt om det går eller så skickas den vidare för åtgärd/besked av specialister. Ifall det är särskilt brådskande så ringer du till supporten.

Särskilt brådskande med anmälan är ifall du misstänker att någon annan person, känd eller okänd, använt din användaridentitet. I så fall gör du så här:

- byt omedelbart ditt lösenord som hör ihop med din användaridentitet
- notera när du senast var inne i IT-systemet
- notera när du upptäckte incidenten
- anmäl omedelbart förhållandet till din närmaste chef som i sin tur ska kontakta ansvariga för informationssäkerhet på IT-kontoret
- dokumentera alla iakttagelser i samband med upptäckten och försök fastställa om kvaliteten på din information har påverkats

Dessa uppgifter behöver du senare när du eller din chef fyller i incidentformuläret på Intranätet.

Incidentrapporterna hamnar hos informationssäkerhetsrådet som bedömer händelsernas omfattning och allvarlighetsgrad samt beslutar om åtgärder.

11.1 ”KONTOFISKE”

Du kan råka ut för att som e-post få en begäran om ditt kontonummer i din bank tillsammans med ditt lösenord. Alla förfrågningar med begäran om lösenord till ditt bankkonto eller användarkonto på e-posten är falska. Falska bluffbrev blir tyvärr vanligare och allt bättre formulerade. Bluffbreven kan påstå att ditt konto tappats bort, uppgraderingar ska göras eller att du har betalat in en för stor summa pengar som de nu vill återföra till ditt konto.

Men kom ihåg, ingen, vare sig banker, försäkringsbolag, statliga myndigheter, TELIA eller kommunens IT-kontor etc frågar någonsin via e-post om ditt lösenord eller önskar veta ditt lösenord till ett bankkonto. Radera sådan e-post.

11.2 VIRUS

Kommunen har programvaror för viruskontroll både i klienterna och på nätverket, men förövarna ligger tyvärr steget före så du kan ändå drabbas av skadlig kod. Om du misstänker att din dator drabbats av virus ska du:

- dra ut nätverkskabeln, men låta datorn vara på
- omedelbart anmäla förhållandet till IT-support, Informationssäkerhetssamordnare, eller till närmaste chef. OBS! Anmälan ska ske per telefon eller besök, inte per e-post

Om du får brev med virusvarning gör inget annat än kontakta IT-support.

USB minnen, handdatorer, digitala kameror, mobiltelefoner mm kan lätt bli virusbärare eftersom dessa kan fungera som ”mellanlagringsstation”. Om du är noggrann med att kontrollera att den dator som du ansluter till kringutrustningen har ett uppdaterat antivirusprogram så har du gjort det som kan och ska göras.

11.3 E-POST, VIRUS, SPAM

Luleå kommun har installerat program som skyddar mot virus och oönskade försändelser (SPAM) i e-posten. Dessa program uppdateras dagligen, men det inträffar tyvärr ändå händelser med e-posten. För att minska riskerna är det viktigt att du tänker på följande:

- öppna inte okända filer
- var försiktig med e-post från okända

- var försiktig med bifogade filer i e-post även från människor du känner, det händer att förfalskare kapar e-postadresser och skickar skadlig kod med epost från betrodd användare
- stäng av alla funktioner som öppnar filer automatiskt
- anmäl omedelbart misstänkt virus till IT-support, anteckna först vad som var smittat av virus
- låt den infekterade filen ligga orörd - spara inte ned den på nätverket
- skicka inte virussmittad e-post vidare
- om du i övrigt är osäker hur på du skall agera, kontrollera alltid med IT-support och skriv en incidentrapport via formuläret på intranätet

Anmälan av virus syftar till att kunna begränsa spridningen, att viruset rensas bort och att en analys kan genomföras av var viruset kommer ifrån.

12 ANVÄNDARENS PERSONLIGA INTEGRITET

Du använder Luleå kommuns informationssystem, nätverk och utrustning och behöver känna till hur uppgifter om dig kan komma att användas av IT-kontoret och din förvaltning.

För att upprätthålla spårbarheten sparas loggar i de flesta system och applikationer. I loggarna kan man exempelvis utläsa när användaren varit inloggad, vilka eventuella förändringar som gjorts och vid vilken tidpunkt.

Loggarna granskas för att upptäcka om system används felaktigt eller otillbörligt eller på ett sådant sätt att det strider mot lagar eller avtal. Systemägaren beslutar om vem som ansvarar för granskningen, hur ofta och på vilket sätt loggarna ska granskas.

Vid misstanke om missbruk av kommunens utrustning eller information så kan förvaltningschef/kontorschef/bolagschef begära loggranskning avseende den användare eller applikation misstanken gäller.

Vid misstanke om brott lämnas ärendet vidare till brottsutredande myndighet, som kan komma att begära ut innehåll i e-postsystem och i hemmakatalog.

Arbetsgivaren kan komma att ta del av innehållet i e-post och andra meddelandesystem om det är nödvändigt för att uppfylla kommunens skyldighet om allmänna handlingars offentlighet. Orsaken kan också vara skälig misstanke om brott, brott mot anställningsavtalet eller av säkerhetsskäl. Uttalad ansvarig person gör då en avvägning mellan arbetsgivarens intressen och individens personliga integritet.

Om du har anmält ett fel eller problem till IT-support kan ibland en tekniker från IT-kontoret behöva fjärrstyra din dator för att lösa felet eller problemet. Teknikern kontaktar dig innan för att meddela detta. För att snabbt kunna avhjälpa dina problem finns det situationer där teknikern kan komma att åtgärda applikationsproblem på din dator även om du inte är vid din dator när teknikern ringer eller om teknikern inte får tag på dig, men det är alltid med din vetskap och godkännande.

I syfte att optimera användandet av nätkapacitet, diskutrymme med mera kan IT-kontoret komma att se över innehållet i hemmakataloger och arbetsrum. Enstaka filer granskas dock inte i dessa fall, utan endast det totala utnyttjade utrymmet.

13 AVSLUTNING ELLER FÖRÄNDRING AV ANSTÄLLNING

När du slutar din anställning ansvarar du för att:

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas
- allt arbetsmaterial du framställt anses vara Luleå kommuns egendom och får inte tas med utan chefs godkännande
- eget privat material som ska behållas flyttas över till en privat USB-sticka eller annat minnesmedium. Därefter raderas det privata materialet
- de behörigheter du fått för åtkomst till kommunens informationssystem avbeställs av din chef till systemägaren
- tömma röstbrevlådan på hälsningsmeddelande och inkomna meddelanden. Observera att det kan ligga kvar meddelanden trots att du inte använder röstbrevlådan.

Av säkerhetsskäl sparas allt material i hemkatalog och e-post i 90 dagar efter avslutad anställning. Det kan inträffa situationer som motiverar att informationen är tillgänglig även en viss tid efter avslutad anställning. När tidsfristen på 90 dagar passerats så raderas exempelvis informationen i din personliga hemkatalog (H:) och din e-post.

Vid längre sjukfrånvaro eller hastigt dödsfall kan material flyttas från användarens lagringsyta på H: till annan åtkomlig yta. Det kan också bli aktuellt med att styra personens e-post till annan medarbetare eller chef. Sådan åtgärd utförs efter begäran om detta från användarens chef.

14 PÅFÖLJDER OCH ÅTGÄRDER

Systemägare ska anmäla avsteg mot riktlinjerna eller brott enligt gällande lagstiftning till närmast beslutsmässig funktion enligt delegationsordning. Saknas tydlig delegationsordning så anmäls det till beslutande politisk organisation inom vilket ansvarsområde applikationen eller nätet sorterar under.

Systemägaren har rätt att vid grundad misstanke om avsteg från riktlinjerna hindra tillgång till IT-resurser. Hindrande av tillgång till IT-resurser får endast utsträckas i tiden till dess att beslut om påföljd fattats av behörig funktion.

IT-kontoret har – som ansvarig för förvaltningsövergripande system och kommunikationsnät – rätt att ingripa om exempelvis kommunikation med extern eller annat internt nät används på fel sätt. IT-kontoret förbehåller sig rätten att bedöma om användning av intern nätutrustning gjorts på ett felaktigt sätt. Om sådan händelse inträffar så meddelas berörd systemägare och systemförvaltare omedelbart.

Om kontrollerna visar på överträdelser av riktlinjer så utreds frågan av utsedd ansvarig, ex v IT-chef. Arbetsgivaren försöker i första hand åstadkomma rättelse genom förtydligande personligt samtal. Vid allvarliga förseelser tillämpas disciplinära åtgärder, och i sista hand avslut av anställning.

Om överträdelser faller in under någon brottslagstiftning så lämnas ärendet till polisiär utredning.

15 EFTERLEVNAD AV ”RIKTLINJER - INFORMATIONSSÄKERHET FÖR ANVÄNDARE”

För att bibehålla ett systematiskt informationssäkerhetsarbete är det viktigt att:

- IT och informationssäkerhetsutbildning är en del av introduktionen för nyanställda
- Närmaste chef säkerställer att samtliga medarbetare vid arbetsplatsen har genomfört DISA-utbildningen minst en gång samt vid alla nyanställningar
- Informationssäkerhet ingår i internkontrollen som ett obligatoriskt kontrollmoment

Säkerhetsanvisningar för mobila enheter

1. Inledning

För att uppnå en trygg och säker hantering av våra avancerade mobiltelefoner i Luleå kommun krävs en enhetlig syn på användningen. Dessa anvisningar ska bidra till att kommunens medarbetare känner trygghet i sin mobilanvändning. Mobiltelefoner och andra mobila enheter likställs med datorer och ska därför skyddas på samma sätt. Mobiltelefonen ska betraktas som ett verktyg i arbetet och det är den anställdes skyldighet att använda den mobila enheten med gott omdöme.

Den största säkerhetsrisken för mobila enheter är fysisk försummelse (stöld eller förlust) och det är därför varje medarbetares ansvar att vara aktsam om sin mobila enhet och förvara den på ett säkert sätt.

Kommunen använder sig av ett administrativt verktyg för en säker och funktionell hantering av kommunens mobila enheter. De avancerade mobila enheterna installeras med en programvara som gör det möjligt att ta kontinuerlig backup på mobilens data, sätta säkerhetspolicys samt att spärra och låsa den mobila enheten vid förlust eller stöld. Denna programvara kommer också att vara nödvändig för att synkronisera din mobila enhet mot kommunens e-postsystem.

Programvaran installeras av IT-kontoret och endast på de enheter som omfattas av kommunens avtal om inköp av mobila enheter.

2. Anskaffning och abonnemang

Anskaffning av mobiltelefon ska ske enligt Luleå kommuns gällande ramavtal ”Mobila enheter med tillbehör och funktionsupprätthållande tjänster”.

Beställning görs via Intranätet från aktuellt standardiserat utbud. Tjänsten nås via intranätet ”Tjänster och Support – Telecom”. Om beställningen innebär avsteg från standardutbudet eller på annat sätt avviker, så samråd direkt med Service & Support, IT-kontoret.

Mobila abonnemang öppnas hos Service & Support, IT-kontoret.

Vid beställning av ska användaren godkänna att man tagit del av dokumentet ”Säkerhetsanvisningar för mobila enheter”. Om beställningen görs av ombud ansvarar denne för att säkerhetsanvisningarna kommer användaren tillhanda. Bifogad bilaga kan användas som extra säkerhetsåtgärd.

Det är viktigt att din mobila enhet har rätt abonnemangsform. En enhet av modell ”smartphone” skall, för att minimera kostnader, ha ett abonnemang där paketerad datatrafik ingår. Fel abonnemang för ej avsedd mobil enhet riskerar onödigt höga kostnader. Service & Support på IT-kontoret är behjälpliga med att öppna rätt abonnemang till vald enhet.

Även om du inte aktivt surfar på den mobila enheten så genererar enhetens olika tjänster datatrafik, vilket gör att abonnemanget kan belastas med höga kostnader om det är ett felaktigt abonnemang.

3. Förlust

Eventuell förlust av mobil enhet ska polisanmälas av användaren. När polisanmälan är gjord kontaktar användaren Service & Support vid IT-kontoret som stöldstänger telefonen, fjärrstyr enheten, låser telefonen och rensar dess information.

4. Lösenordsskydd

Den mobila enheten ska lösenordskyddas så att den är låst när skärmsläckaren är aktiv. Enkla koder, tex 1111, 1234, de fyra sista siffrorna i personnumret, anknytning etc. ska inte användas.

5. Synkronisering av E-post och kalender

Synkronisering av e-post och kalender får endast ske med av kommunen godkänd mobil enhet, se kap. 2 ”Anskaffning och abonnemang”. Synkronisering av privata enheter tillåts ej. För e-post kan man ställa in hur mobilen ska hämta ny e-post. Det säkraste, också ur ett integritetsperspektiv, är att använda sig av pull-teknik dvs. att man hämtar ny e-post manuellt. Service & Support vid IT-kontoret ger stöd och hjälp för de användare som ska synkronisera sin mobiltelefon.

6. Datatrafik utomlands

Vid vistelse utanför Sverige ska all mobil datatrafik stängas av. Detta gäller för såväl mobiltelefoner som läsplattor. Mobil datatrafik ska endast öppnas för trafik vid behov. Även om du inte aktivt surfar på den mobila enheten så genererar enhetens olika tjänster datatrafik, vilket gör att abonnemanget kan belastas med höga kostnader. Mobil datatrafik är mycket dyrare utomlands än i Sverige så du måste vara vaksam på hur mycket dessa tjänster används.

Fasta månadsavgifter för mobil datatrafik gäller inte utanför Sverige.

7. Installation av applikationer (appar)

Varje användare av mobil enhet ansvarar personligen för inköp och nedladdning av applikationer för den mobila enheten.

Endast publicerade applikationer från Google Play Butik och AppStore får laddas ned. Tänk på att vissa applikationer begär tillgång till och vill synkronisera data på din mobiltelefon, ex kontaktuppgifter, e-post, bilder m m.

8. Nedladdning av filer mm

Det är medarbetarens ansvar att vara aktsam och inte öppna länkar, filer eller acceptera förfrågningar där syftet eller avsändaren är okänd eller otydligt angiven. Privatkopierade spel eller liknande får inte installeras på den mobila enheten då dessa kan innehålla skadlig kod.

9. Antivirus

Som användare behöver du inte själv förse din mobila enhet med antivirusprogram eftersom samtliga mobila enheter är utrustade med antivirusprogram som tillhandahålls av IT-kontoret. OBS! Gäller endast Android-enheter.

10. Anslutning via publika nätverk och Bluetooth

För att undvika omedveten kommunikation med omvärlden bör den trådlösa nätverksanslutningen på din mobil vara avstängd när den inte används. För att ytterligare minimera att den mobila enheten kan smittas av skadlig kod bör även Bluetooth-anslutningen stängas av när den inte används. Acceptera endast tillförlitliga anslutningar.

11. Kryptering

För att hantera känslig information som t ex personuppgifter, kreditkortsuppgifter, inloggningsuppgifter eller liknande på ett säkert sätt, ska enhetens krypteringsfunktion aktiveras. För att kryptera mobila tjänster som hanterar känslig information ska protokollet https: användas. IT-kontorets avdelning Service & Support, är behjälplig med instruktioner.

12. Lagring av information

Användningen av s.k. molntjänster, ex Dropbox och I-Cloud bör undvikas helt för lagring av kommunal information. Om du ändå använder dig av en sådan tjänst, tänk på att

tjänsteleverantörens villkor innebär att informationen kan återanvändas för andras eller leverantörens egna syften.

Observera att personuppgifter och integritetskänslig information inte får lagras i molntjänster enligt personuppgiftslagen.

13. Övrigt

Den mobila enhetens originalkonfiguration får ej modifieras/ändras genom sk jailbreaking och rootning. Om detta sker kommer den mobila enheten att spärras.

Bilaga – Ansvarsförbindelse

Datum	
Namn på mobiltelefoninnehavare	
Mobilnummer	
Arbetsplats	
Ansvarsnummer	

☐ **Jag har tagit del av dokumentet ”Säkerhetsanvisningar för mobila enheter” och förbinder mig härmed att agera utifrån dessa.**

……..
(Underskrift av mobiltelefoninnehavaren)

…….
(Underskrift av ansvarig chef)