S

Reviderad IT-säkerhetsinstruktion för Norrmalms stadsdelsnämnd

Innehållsförteckning **Sid**

1 Inledning

Syftet med denna instruktion är att beskriva de regler och rutiner som gäller för informationssäkerheten vid Norrmalms stadsdelsförvaltning.
De störningar som kan inträffa, kan medföra allvarliga ekonomiska och andra konsekvenser både för verksamheten och för medborgarna.
Denna instruktion är framtagen utifrån stadens policy och regler för informationssäkerhet och vänder sig till all personal vid Norrmalms stadsdelsnämnd som är IT-användare. Instruktionen ska finnas tillgänglig för alla användare. Verksamhetsansvarig chef ansvarar för att personalen tagit del av och tillämpar instruktionen.

Den som upptäcker brister i säkerheten eller saknar regler/rutiner är skyldig att kontakta sin chef eller IT-säkerhetssamordnarna.

Syftet med arbetet när det gäller informationssäkerhet är att förebygga störningar samt säkerställa att IT-verksamheten bedrivs under lagenliga och säkra former. Säkerhetsarbetet ska primärt inriktas på förebyggande åtgärder.

Till instruktionen finns 8 bilagor.
Den reviderade instruktionen med bilagor har godkänts av Norrmalms stadsdelsnämnd 2003- .

1.1 Ansvar och organisation

Stadsdelsnämnden är ytterst ansvarig för IT-verksamheten inom sitt område och skall därför också besluta om regler och anvisningar för IT-säkerheten. Nämnden bör löpande följa upp IT-verksamhet, IT-säkerhet och övrig intern kontroll och behöver därför en gång per år få en rapport över IT-säkerhetens status.

Ansvaret för IT-säkerheten är kopplad till verksamhetsansvaret. Det innebär att verksamhetsansvarig chef svarar för IT-säkerheten inom sitt verksamhetsområde. Informationssäkerhet ingår som en integrerad del i chefsansvaret och det ansvar varje anställd har för att utföra sitt arbete på ett sätt som överensstämmer med Stockholms stads verksamhet och mål.
Stadsdelsdirektören har det förvaltningsövergripande ansvaret för IT-säkerheten.

Inom förvaltningen finns två IT-säkerhetssamordnare. Dessa ansvarar för att sprida kunskap om regler, metoder och tekniker avseende IT-säkerhet. IT-säkerhetssamordnarna sammanställer säkerhetsrapporter till stadsdelsnämnden och förvaltningsledningen. Säkerhetsarbetet sorterar under Stadsmiljö- och planeringsavdelningen.

För ytterligare information om IT-säkerhetsansvaret hänvisas till den IT-säkerhetsorganisation för Norrmalms stadsdelsnämnd som finns i bilaga 1.

1.2 Personal och säkerhet

Anställning	Uppgifter som lämnas i platsansökningar skall kunna verifieras och referenser skall tas i erforderlig omfattning En kort information om den anställdes informationssäkerhetsansvar skall lämnas vid anställning. Personal som kommer i kontakt med sekretessbelagda handlingar skall informeras om Sekretesslagen och dess innehåll. För viss verksamhet gäller from 2001-01-01 Lag om registerkontroll.
Utbildning	Alla användare liksom konsulter och övriga tredjepartsanvändare, skall få anpassad och uppdaterad utbildning i vilka riktlinjer och rutiner som gäller vid förvaltningen.
Incident-rapportering	Alla användare skall rapportera relevanta incidenter till IT-enheten eller till IT-säkerhetssamordnarna, vilka i sin tur rapporterar vidare till stadsdelsdirektören och till stadens IT/informationssäkerhetschef. Det kan gälla virusangrepp, intrångsförsök, felaktig hantering av personuppgifter, inbrott/inbrottsförsök eller funktionsfel som kan ha uppstått pga oegentligheter.
Avslut/ ändring av arbetsuppgifter	För de fall när personer slutar sin anställning eller övergår till annan enhet/andra arbetsuppgifter inom förvaltningen skall finnas rutiner som styr avveckling/förändring av tillgång till såväl lokaler som IT-system och information.
Uppsägning/ övertalighet	Användare med högre behörigheter till lokaler och system bör fråntas dessa högre behörigheter omedelbart i samband med underrättelsen om förändringarna. Normala användarbehörigheter kan bibehållas så länge personen är i tjänst. Möjlighet till riktad loggning skall beaktas.
Över-trädelser	Överträdelser av förvaltningens säkerhetsregler hanteras av verksamhetsansvarig chef.

1.3 Vad omfattar begreppet IT-säkerhet?

Säkerhetsarbetet omfattar alla åtgärder vars samlade effekt är att förebygga och begränsa konsekvenserna av störningar för informationshantering för verksamheterna inom Norrmalms stadsdelsförvaltning.

1.4 Definitioner

IT-säkerhet kan delas in i följande områden:
(källa; Informationstekniska Standardiseringen, ITS 6)

Informationssäkerhet	säkerhet vid hantering av information avseende önskad tillgänglighet, kvalitet, sekretess och spårbarhet
IT-säkerhet	IT-säkerhet kan uppdelas i ADB-säkerhet(Datasäkerhet) och kommunikationssäkerhet
Datasäkerhet	Säkerhet avseende skydd av data och system mot

	obehörig eller oavsiktlig förändring eller störning vid databehandling
Kommunikationssäkerhet	Säkerhet i samband med överföring av information eller styrsignaler

2 Rättsliga krav på IT-användningen

2.1 Lagstiftning

Det finns sedan lång tid lagar och andra författningar som reglerar dokument- och informationshantering i offentliga myndigheters verksamhet. Minimikraven på förvaltningens informationssäkerhetsnivå ställs genom gällande lagar och förordningar.

Regleringen har bl. a. till syfte att

- garantera att verksamheten sker i demokratiska former
- garantera medborgarna insyn i och kontroll av förvaltningen
- förhindra maktmissbruk och garantera medborgarnas rättssäkerhet
- skydda den enskildes integritet.

De viktigaste lagarna för att uppnå dessa syften är;
Tryckfrihetsförordningen (SFS 1949:105), Sekretesslagen (SFS 1980:100), Lagen om kommunal redovisning (SFS 1997:614), Datalagen (SFS 1973:289), Arkivlagen (SFS 1990:782), Lag om upphovsmannarätt till litterära och konstnärliga verk (SFS 1960:729, Lag om skydd av företagshemligheter (SFS 1990:409), Personuppgiftslagen (SFS 1998:204) samt de olika speciallagar som styr verksamheten.

Arkivlagen reglerar hur allmänna handlingar och därmed även elektroniskt lagrad information, skall förvaras och hur gallring får ske.

Tryckfrihetsförordningen, sekretesslagen och datalagen har regler som direkt styr IT-användningen i syfte att garantera allmänhetens rätt till insyn och att skydda den enskildes integritet.

I lagen om kommunal redovisning redovisas hur bokföring skall ske, räkenskapsmaterialets bevarande och arkivering.

I lagen om upphovsmannarätt till litterära och konstnärliga verk har skrivits in bestämmelser om bl a datorprogram.

Lagen om skydd av företagshemligheter: med företagshemlighet avses sådan information om affärs- eller driftsförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för denne i konkurrenshänseende.

Personuppgiftslagen: lagen omfattar all automatiserad behandling av personuppgifter och manuell behandling av personregister.

Lagen innehåller bestämmelser om när behandling av personuppgifter är tillåten. I bilaga 3 till denna instruktion finns en rutinbeskrivning avseende hantering av personregister vid Norrmalms stadsdelsnämnd. PUL-ansvariga kan även bistå med ytterligare information.

För ytterligare fördjupad information om lagarna hänvisas till lagtexten eller stadens regler och policy för informationssäkerhet.

2.2 Analys av befintliga och planerade system

Inga nya system får tas i bruk utan att det föregås av en analys av hur systemet förhåller sig till tryckfrihetsförordningens, sekretesslagens, arkivlagens personuppgiftslagens och datalagens bestämmelser och andra regler som styr verksamheten. I samband med denna analys skall alltid IT-säkerhetssamordnarna informeras.
Inom Norrmalms stadsdelsnämnd upphandlas vissa verksamheter i konkurrens. I de fall utfallet av upphandlingen innebär att verksamheten skall skötas av utomstående entreprenör bör vissa IT-säkerhetsaspekter beaktas. Om den nye utföraren ges tillgång till system inom förvaltningen som innehåller personregister bör avtal träffas om att förvaltningen har rätt att kontrollera IT-säkerheten hos utföraren.

3 Fysisk och miljörelaterad säkerhet

3.1. Tillträdesskydd

Utrymmen där viktig utrustning för IT-driften förvaras skall ha ett starkt tillträdesskydd så att endast personer som har till uppgift att arbeta med utrustningen kommer åt densamma. Med IT-utrustning avses datorer, kommunikationsutrustning, skrivare, bandstationer, konsoler etc. Vidare ingår datamedia såsom disketter, magnetband, CD-ROM-skivor och dylikt.

IT-chefen har ansvar för att skriftliga regler för vem som har tillträde till utrustningen upprättas och underhålls. Nyckel-, kort- och kodinnehav skall vara förtecknade. Nycklar och passerkort skall förvaras i säkerhetsskåp.
Nyckelschema och rutiner för utlämning av nycklar med kvittoförfarande skall tillämpas.
Utomstående, exempelvis tekniker skall ha tillträde till serverrum endast om bevakning sker. Sådana besök loggas och för okända gäller legitimationstvång. I loggen anges datum och tid för besöket samt ärendets art.

3.1.2 Brand-, värme- och vätskeskydd

Nätservers, kommunikationsutrustning och dyl. som är avsedda för ett flertal användare skall vara placerade på ett ur brandsynpunkt betryggande sätt. Det innebär t. ex. placering i ett rum utformat som en brandcell avskild från omgivningen med lägst brandklass A60[1] samt försedd med rökdetektorer och släckningsutrustning.

[1] A60 innebär att brandcellen skall motstå en omgivande brand minst 60 minuter.

Utrustning skall vara placerad så att den inte riskerar att utsättas för vätskeläckage, korrosiva gaser[2], damm, smuts, avmagnetisering etc.

Datamedia som innehåller information (disketter, band och CD-ROM-skivor) och systemdokumentation skall förvaras i brandsäkra skåp. Förvaring i vanliga plåt- eller kassaskåp ger inte tillräckligt brandskydd.

Verksamhetskritiskt material som är pappersburet eller datamedia skall förvaras i brandklassat säkerhetsskåp i låst utrymme. Reservutrustning skall förvaras i låst utrymme med begränsad tillgänglighet. Detta innebär att endast auktoriserad personal har tillgång till utrymmet.

3.1.3 Lokal för serverrum

Rummet skall vara utrustat med säkerhetsdörr. Väggarna skall vara förstärkta så att de är svåra att forcera, golvet utformat så att förekomsten av statisk elektricitet reduceras. Dörrar och väggar bör hålla godkänd brandklass och genomföringar till lokalen rökgastätas. Det är viktigt att serverrummet har ett gott skydd mot vattenskador och vattenläckage.
Begränsad och kontrollerad tillgänglighet skall råda, rummet skall hållas fritt från onödig utrustning. Regelbunden städning skall ske.
Temperaturen i rummet får inte överstiga 20 grader. Lokalen skall vara skyddad med inbrottslarm, brandlarm och temperaturlarm.
Manuell brandsläckare och tillgång till telefon skall finnas i rummet.

3.1.4 Service av extern servicegivare

Service av utrustning och program skall i varje enskilt fall påkallas av och utföras under överinseende av egen personal.
Så kallad ”remote service”, d.v.s. service av maskin- och programvaror via telenätet, får endast utföras om känslig information görs oåtkomlig för servicegivaren. Stående lösenord och löpande åtkomst får inte förekomma.

Databärare (d.v.s. hårddisk, magnetband o dyl.) som innehåller känslig information får inte sändas till leverantör för reparation, utbyte eller liknande om inte innehållet har överskrivits, avmagnetiserats eller är krypterat.

3.2 Placering av utrustning

Utrustning där känslig information kan läsas (bildskärm, skrivare, fax) skall skyddas så att obehöriga inte kan ta del av informationen. Detta kan ske antingen genom placeringen av utrustningen eller för bildskärmar att skärmsläckarfunktion med lösenord aktiveras omgående då bildskärmen lämnas utan uppsikt.

3.3 Stöldskydd

All datorutrustning tillhörande Norrmalms stadsdelsförvaltning skall vara stöldskyddsmärkt. Samtliga persondatorer skall stöldskyddsmärkas.

[2] Gaser som gör att utrustningen utsätts för rostangrepp.

Alla lokaler där datorutrustning förvaras skall vara inbrottslarmade under icke arbetstid. I lokaler där utrustning förvaras på nedre botten skall fönstren vara larmade alternativt försedda med galler.
Tillgreppsutrustning som t ex boxar skall övervägas om skalskydd eller miljö är sådan att tillgrepp kan ske på ett enkelt sätt.
Bärbara persondatorer bör vara försedda med wirelås för att förhindra tillgrepp av typen ”smash and grab” vid arbete utanför ordinarie arbetsplats.

När det gäller publika miljöer (medborgarservice m.m.) skall administrativa åtgärder vidtagas för att motverka anonym användning av stadens tillhandahållna datorer. Rutiner för ID-uppvisande vid datorlån skall finnas för detta ändamål.

3.4 Makulering och utrangering

Datamedia skall destrueras eller utplånas på sitt informationsmaterial på ett tillförlitligt sätt innan det makuleras eller utrangeras.

Datamedia får endast friställas efter överskrivning eller efter avmagnetisering. Detta gäller oavsett i vilken datormiljö datamedia har framställts. Observera att ”delete” eller omformatering av diskett inte är tillräckligt.
IT-enheten kontaktas vid behov.

Datamedia som har blivit obrukbar eller av annan anledning måste kasseras skall förstöras.

4. Kommunikation och drift

4.1. Datakommunikation

4.1.1 Datakommunikation

I samband med att information överförs genom datakommunikation uppkommer risker för avlyssning eller förändring av den överförda informationen.

Bärbara datorer och datorer som ej är anslutna till nätverket och som hanterar känslig information skall ha krypteringsskydd på hårddisken.

Behov av skydd för röst- fax- och videokommunikation skall beaktas.

4.1.2 Modem

Inga modem får kopplas till enskilda persondatorer som är anslutna till stadens nät. All extern kommunikation skall ske via stadens gemensamma modempool.

4.1.3 Brandvägg

All extern trafik baserad på kommunikationsprotokollet TCP/IP skall gå via brandvägg och filtreras utifrån verksamhetsbehoven.

För de verksamheter som kräver på öppningar som inte kan accepteras med hänsyn till den totala säkerhetsbilden skall dessa funktioner hanteras via DMZ (de-militariserad zon, en egen brandväggsväg) eller annan likvärdig lösning.

4.1.4 Fjärråtkomst

All uppringd analog kommunikation skall ske med hjälp av engångslösenord, som genereras för varje tillfälle. ISDN/ADSL-kommunikation skall ske med hjälp av krypterat lösenordsutbyte mellan routrar.

4.1.5 Stadsnät/Internet

Med nuvarande lösning dvs ett slutet administrativt nät, får inga okontrollerade sammankopplingar mot Internet göras. Detta innebär att den publika delen av stadsnätet skall hållas åtskild från den administrativa delen.
För att undvika att publika datorer används i syften som strider mot stadens etiska regler ska rutiner finnas för ID-uppvisande vid datorlån.

Material som lyder under sekretess ska aldrig publiceras på Internet eller på Intranätet.
Internet ger möjlighet att länka till annan information än stadens egen t ex andra kommuner och statliga verk men också informationslämnare utanför den offentliga sektorn. Varje deltagare/informationslämnare inom förvaltningen ansvarar för att inga länkar upprättas som leder till verksamheter eller information som förvaltningen inte vill associeras med.
När det gäller användning av Internet inom förvaltningen hänvisas till ”IT-strategi för Norrmalms stadsdelsnämnd”.

4.1.6 Elektronisk post

Anställda inom förvaltningen får inte skicka sekretessbelagda eller integritetskänsliga uppgifter med extern e-post utan adekvat krypteringsskydd.
Mottagna sekretessbelagda eller integritetskänsliga uppgifter skall tas ut på papper och raderas ur de elektroniska postsystemen.
Replikering (vidarebefordran) av elektronisk post till annan brevlåda får endast ske om krav på diarieföring kan tillgodoses och en i övrigt god offentlighetsstruktur kan upprätthållas vid mottagandet.
Detta innebär bland annat att generell vidarebefordran till publika brevlådor exempelvis Hotmail-tjänster inte är tillåtet.
I övrigt hänvisas till förvaltningens regler för e-posthantering, se bilaga 7.

4.2 Datavirus

Ett virus i datasammanhang är ett program som är konstruerat för att dels spridas genom ”smitta”, dels åstadkomma någon form av skada. Skadan som viruset åstadkommer kan variera. Ett exempel är att virus snabbt tar allt tillgängligt utrymme i datorn i anspråk och får all övrig verksamhet att bryta samman. Andra virus kan radera innehållet på datorns hårddisk.

Viruset kan finnas ”osynligt” i datorn en längre tid innan det aktiveras. Vanligen aktiveras viruset ett visst datum, en speciell tid eller av ett visst kommando.

Anti-virusprogram skall installeras och kontinuerligt uppdateras på samtliga persondatorer på förvaltningen. IT-enheten kan hjälpa till vid frågor om detta. Privata program och spel får inte användas. Endast program godkända av förvaltningen får användas.

4.3 Drift

4.3.1 Driftsrutiner

Det skall finnas en förteckning över all maskin och programvara
och för varje system skall finnas dokumenterade och uppdaterade driftsrutiner. Ansvaret för detta har den lokala systemförvaltaren. I de fall systemförvaltarskapet inte ligger på stadsdelsnämnden skall dokumentation finnas om systemansvarigas roll och ansvar.

För driften av förvaltningens nätverk och system som lagras på servern skall finnas dokumenterade driftsrutiner. Ansvaret för detta ligger på IT-chefen.

Kapacitetsbehov av lagringsutrymme, processer m.m. skall följas upp och uppskattning av framtida behov skall genomföras

Operatörsarbetet skall alltid loggas så att handlingar av personer med hög behörighet kan spåras vid behov.
System och rutiner för ändringshantering skall finnas.
Hårdvaruleverantörers specifikationer för driftmiljöer skall följas.

4.3.2 Störning, system och driftsfel

Det skall finnas rutiner, manuella och/eller maskinella, för att rapportera om störningar/system och driftsfel av olika slag. Informationen kan ligga till underlag för senare förbättringar.

4.3.3 Dokumentation

Varje system och funktion skall vara dokumenterad på ett fullständigt och så likartat sätt som möjligt så att systemförvaltning och systemanvändning förenklas. Relevanta drifts och systemdokumentationer skall finnas. Original bör placeras i säkerhetsskåp.
Minst en aktuell kopia av handlingar och andra dokument för systemens användning och drift bör förvaras väl skyddade och åtskilda.

Alla användare bör ha tillgång till en aktuell användardokumentation för vart och ett av de system som han/hon använder.

4.3.4 Personberoende

Personberoende skall så långt möjligt undvikas genom utbildnings- och arbetsbytesprogram. Detta avser såväl IT-enheten som övriga användare.

4.3.5 Leverantörsberoende

Beroende av viss leverantör skall undvikas. Om det inte kan ske bör åtgärder vidtas som kan mildra eventuella effekter om t.ex leverantören skulle försvinna från marknaden. I samband med köp av programprodukter skall man undersöka om leverantören kan ställa garantier om följsamhet vid förändringar i den tekniska bearbetningsmiljön.

4.3.6 Säkerhetskopia och backup

Säkerhetskopia för skydd mot extraordinära störningar. Säkerhetskopia skall förvaras i byggnad åtskild från driftlokalen. Säkerhetskopior omfattar operativsystem, hjälpprogram och dokumentation samt vecko- och månadsbackuper av information på servern. Ny säkerhetskopia skall alltid tas av operativsystem, hjälpprogram och dokumentation när någon förändring skett. Säkerhetskopia vilken motsvarar verksamhetens krav på rimliga återgångstider till driftssituation skall alltid finnas.
Backup och säkerhetskopia skall förvaras så att avsiktlig eller oavsiktlig förändring, förstöring eller spridning av informationen förhindras.

Rutin för återlagring av driftsbackup och säkerhetskopia skall vara beskriven i driftsdokumentationen. Återlagringen skall testas.

Varje dygn görs en totalbackup för förvaltningens nätverk. Det innebär att såväl programvaror som information kopieras. Vecko- och månadsbackuper sparas åtskilt som säkerhetskopior.

För information som lagras på persondatorns hårddisk ansvarar varje användare själv för driftsbackup och säkerhetskopiering.

4.4 Säkerhet i WEBB-tjänster

En Webbtjänst är en eller flera applikationer, åtkomliga för en webbläsare från intranätet eller Internet.
Dessa drivs på en server med webbserverprogram.
Vissa säkerhetsaspekter måste beaktas för att förhindra att någon obehörig kommer åt server och att data ändras.

4.4.1 Skalskydd

Webservern skall finnas i lämpliga lokaler. Serverrummet skall vara låst och endast behörig personal skall ha tillträde.

4.4.2 Placering av webbserver

Stadsledningskontorets IT-avdelning har etablerat en s.k. DMZ-zon för access av webbapplikationer från Internet. I första hand skall detta nät användas för etablering av webbtjänster.
Placering av webbtjänster på stadens/förvaltningens publika nät är inte tillåten.

4.4.3 Serveruppsättning

En webbserver är alltid mer eller minde åtkomlig från Internet. Därför skall installation, antal aktiva tjänster m.m. minimeras för att försvåra för ovälkomna besökare. Patchar och servicepacks som berör säkerheten skall installeras när de finns till förfogande.
Webbservern får aldrig lämnas påloggad. Ingen applikation som kan vara åtkomlig från Internet får länkas direkt in i det administrativa nätet.

4.4.4 Kryptering

Presentation av data som kan bedömas som känsligt, liksom applikationer som på ett eller annat sätt har en uppdaterande funktion, skall krypteras med hjälp av SSL (Secure Sockets Layer)

4.4.5 Backup

Ansvarig för respektive Webb-tjänster skall fastställa behovsfrekvensen.

4.4.6 Brandvägg

Webbservern placeras alltid bakom en s.k. brandvägg för att försvåra för ovälkomna besökare.

4.4.7 Behörigheter

Alla användare som skapar eller tillför information skall använda personliga användarkonton. Generella konton accepteras inte.
All uppdatering bör ske på stadens administrativa nät.

4.4.8 Publicering av data

All publicering skall ske via ett s.k. stagningssystem. All uppdatering direkt på webbserver skall undvikas.

4.4.9 Databaser och applikationer

Åtkomst till databaser och applikationer kan ske via en PKI-lösning eller att informationen presenteras via databasserver placerad på DMZ-nätet .
Data som presenteras direkt skall finnas på servrar, placerade på nät som kontrolleras av förvaltningen.

5. Kontinuitets- och avbrottsplanering

5.1 Vad är kontinuitets och avbrottsplanering

Med K/A-planering avses planering mot störningar som är så svåra att de inte kan åtgärdas inom ramen för de normala rutinerna och resurserna.

5.1.2 K/A-planering vid Norrmalms stadsdelsförvaltning

Stadsdelsförvaltning skall ha en övergripande Kontinuitets- och avbrottsplanering. Den ska omfatta åtgärder och prioriteringar för större dataavbrott i förvaltningens verksamhet.

Verksamhetsansvariga skall ansvara för att K/A-planer som skall träda i kraft vid allvarligt/långvarigt datorbortfall vid den egna verksamheten utformas och dokumenteras. Såväl reservrutiner som K/A-planer skall hållas aktuella och övas för att med kort varsel kunna sättas in. Målet för planerade åtgärder är att kunna upprätthålla verksamheten i nödvändig omfattning utan kostsamma stillestånd.

6. Styrning av åtkomst

6.1 Behörighetstilldelning och behörighetskontroll

Varje medarbetare skall ha den behörighet som krävs för att kunna utföra sina arbetsuppgifter. Det skall finnas skriftliga regler för vem som skall ha tillgång till en viss information samt på vilket sätt det skall ske.

Verksamhetsansvarig chef skall tillse att medarbetare ges rätt behörighet samt att behörigheten spärras då den inte längre behövs. Rutiner för tilldelning, ändring och borttag av behörigheter återfinns i bilaga 4.

6.2 Uppföljning av behörigheter

En gång per kvartal skall behörigheterna inom förvaltningen kontrolleras. Kontrollen genomförs av IT-enheten, som går igenom befintliga behörigheter med verksamhetsansvarig chef.
Utöver detta skall stickprov tas med oregelbundna intervaller.

6.3 Lösenordshantering

Lösenorden skall vara individuella och hemliga. Ett lösenord får inte överlåtas eller tillfälligt lånas ut. Lösenorden skall vara minst 6 tecken långa och bestå av En blandning av alfa-numeriska tecken. Lösenordet får inte medge versionsuppdatering exempelvis april 1, april 2 etc.

Lösenord skall kunna bytas när som helst av användaren. Periodiskt byte bör ske minst var 30:e dag och påkallas automatiskt av behörighetskontrollsystemet. Lösenord skall inte gå att återanvända inom 13 månader.
Lösenord får inte synas på skärm eller utskrift.

För varje datorarbetsplats skall finns en s.k. skärmsläckningsfunktion som innebär att man efter en viss tids inaktivitet måste ange rätt lösenord för att kunna fortsätta arbetet. Funktion skall också finnas för att spärra användare efter tre misslyckade inloggningsförsök.

6.4 Loggning och uppföljning

Behovet av loggning och uppföljning av loggar/analys skall fastställas efter verksamhetens behov och genomförd klassificering.
Loggning och analys skall genomföras regelbundet när det gäller obehöriga åtkomstförsök till resurser. (nät, information m.m.)
Maximalt tre felaktiga försök till påloggning skall vara tillåtet. Därefter låses användaridentiteten.
Låsning av användaren pga inaktivitet skall ske efter 60 dagar där så medges.
Åtkomstförsök med felaktiga identiteter eller lösenord och andra upptäckta avvikelser mot behörighetsreglerna skall registreras. Avvikelserna skall redovisas för den chef som beviljar behörigheter till den ”angripna” informationen.

Uppföljning av säkerhetsregler är viktigt för att kontrollera att nivån på säkerheten blir den avsedda. Förvaltningens systemrepresentanter (bilaga 1) svarar för att rutinerna för uppföljning är tillräckliga. Huvudmomenten i uppföljningen är loggning och analys.

Loggningen skall ge underlag för kontroll av att användarna håller sig till tilldelade arbetsuppgifter och att behörighetsfunktioner fungerar på avsett sätt, samt ge underlag för beslut om förändringar i behörighetstilldelningar.

Vidare skall loggningen vara avskräckande mot obehörig användning och på så sätt ge ett skydd i sig. Den skall dessutom kunna utgöra ett utredningsunderlag, eventuellt en lång tid efter att en händelse inträffat, både vid interna och polisiära utredningar.

Alla loggdata måste skyddas mot obehörig förändring eller borttag. Därför skall följande principer tillämpas:

Personer som har behörighet att påverka vitala funktioner (system-, nätverks- eller behörighetsadministration) skall inte ha behörighet att radera loggar eller förändra funktioner som styr loggningen.

Loggar skall inte kunna förändras utan endast raderas. Raderingen skall samtidigt ge upphov till en ny loggpost.

Rutiner för loggning och analys av loggdata skall vara dokumenterade. Loggning och analys får inte innebära intrång i de anställdas integritet.

6.5 Hantering av behörigheter till stadens IT-system för vikarier och tillfälligt anställda

Det har på senare tid blivit allt vanligare att inhyrd personal anlitas som extra personal i verksamheterna, samt att hela verksamheter privatiseras eller läggs ut på entreprenad.

Förvaltningen har dock även i dessa fall kvar det grundläggande ansvaret för de berörda kärnverksamheterna. Detta innebär att om en entreprenör eller motsvarande lämnar sitt uppdrag har förvaltningen skyldighet att se till att verksamheten kan fortsätta med bibehållen kvalitet när det gäller informationen. Medborgarna bör kunna lita på att samma regler för säkerhet och integritet gäller oavsett om det är förvaltningen eller en entreprenör som hanterar information om dem.

För att vikarier och inhyrd personal skall kunna utföra sina uppdrag krävs att vederbörande får tillgång till de datasystem som används i den aktuella verksamheten. Vikarier bör ges behörighet enligt de regler som gäller för övriga anställda
Om tidsintervallerna mellan vikariaten blir långa spärras behörigheterna då de ej används. Rutiner för behörighetstilldelning beskrivs i bilaga 4.

7. Systemutveckling och systemunderhåll

7.1 Systemutveckling

Allt arbete med att ta fram och använda system skall ske i enlighet med en fastställd systemutvecklingsmodell. Under utvecklingsarbetet bör efter hand som de färdigställs kravspecifikation, systemspecifikation och det färdiga systemet granskas ur säkerhetssynpunkt.

Det skall finnas skriftliga instruktioner för hur ett system eller dess delar förs över från utvecklings- och testfas till driftfas, såväl vid första driftsättning som efter systemförändringar.

7.2 Sårbarhetsanalys

Sårbarhetsanalyser skall genomföras i syfte att utröna vilka hot som ett system kan vara utsatt för och ge en konsekvensbeskrivning och förslag på åtgärder som kan vidtas för att ge skydd mot dessa hot.

7.3 Säkerhetsuppföljning

Säkerhetsuppföljning kan ske exempelvis genom:
- intern uppföljning med eller utan hjälp av IT-stöd
- internrevision
- traditionell uppföljning med hjälp av externa konsulter

- attacksimulering av externa konsulter

Förvaltningsledningen, IT-säkerhetssamordnarna eller IT-chefen kan vara initiativtagare till säkerhetsuppföljningen.

7.4 Programtest

Alla program, såväl anpassade standardprogram som egenutvecklade program, skall genomgå tester som fastställer att de utför specificerade funktioner på ett tillfredsställande sätt innan de får tas i drift.

Motsvarande gäller även för program som skall sättas i drift efter en programändring.

7.5 Indata/Utdatakontroller

Funktioner för automatisk kontroll av in- och utdata skall så långt det är praktiskt möjligt ingå i de system som tar emot eller lämnar ifrån sig information. Kontrollen bör exempelvis ske med avseende på rimlighet, fullständighet etc.

7.6 Registervård

Det skall finnas tillförlitliga funktioner för registervård. Speciellt skall rättnings- och rensningsfunktioner beaktas.

7.7 Utbildning

Utbildning av systemanvändare skall ske vid systeminförande och vid förändring av systemet. Plan skall också finnas för utbildning av nytillkomna användare.

Bilagor:

Bilaga 1	IT-säkerhetsorganisation för Norrmalms stadsdelsnämnd
Bilaga 2	IT-säkerhetshandledning för användare
Bilaga 3	Rutiner avseende personregister
Bilaga 4	Rutin för behörighetstilldelning till Norrmalms lokala nätverk samt stordatorsystem
Bilaga 5	Informationsklassning
Bilaga 6	Regler och rutiner för hantering av hemlig handling
Bilaga 7	E-postregler för Norrmalms stadsdelsförvaltning
Bilaga 8	Regler för förvaltningens bärbara datorer