



IT-SÄKERHET

NORRMALMS STADSDELSFÖRVALTNING

MARS 2007

RIKTLINJERNA OMFATTAR:

ALLA ANSTÄLLD INOM NORRMALMS STADSDELSFÖRVALTNING



INLEDNING OCH OMFATTNING.....	3
INLEDNING	3
OMFATTNING.....	3
KLASSIFICERING AV INFORMATION	3
KONTINUITETS- OCH AVBROTTSPLANERING	3
SÄKERHETSUPPFÖLJNING	3
IT-SÄKERHETSORGANISATION FÖR NORRMALM	4
NORRMALMS STADSDELSNÄMND	4
STADSDELSDIREKTÖR.....	4
FÖRVALTNINGENS SYSTEMREPRESENTANT FÖR ÖVERGRIPANDE SYSTEM.....	4
SYSTEMFÖRVALTARE FÖR LOKALA SYSTEM	4
IT-SÄKERHETSSAMORDNARE.....	4
IT-CHEF	5
ANVISNINGAR FÖR HANTERING AV INFORMATION VID SEKRETESS	6
HANTERING AV ARBETSMATERIAL	7
PLACERING AV UTRUSTNING	7
STÖLDSKYDD.....	7
PERSONAL OCH SÄKERHET	7
ANSTÄLLNING	7
AVSLUT/ÄNDRING AV ARBETSUPPGIFTER	8
UPPSÄGNING/ÖVERTALIGHET	8
ÖVERTRÄDELSER.....	8
ANVÄNDARUTBILDNING	8
SÄKERHETSINCIDENTER OCH FUNKTIONSFEL.....	8
INCIDENTRAPPORTERING	8
FYSISK SÄKERHET	10
BÄRBARA DATORER	10
FÖRVARING AV BÄRBARA DATORER	10
SÄKERHETSKOPIERING	10
DISTANSARBETE	10
ARBETE UTANFÖR DEN EGNA ARBETSPLATSEN.....	10
KOMMUNIKATION	11
DATAKOMMUNIKATION.....	11
MODEM	11
FJÄRRÄTKOMST.....	11
DOKUMENTATION.....	11
LOGGHANTERING	11
SÄKERHETSKOPIERING	11
DATAVIRUS OCH SKADLIGA PROGRAM.....	11
SKYDD MOT SKADLIGA PROGRAM	11
STYRNING AV NÄTVERK.....	12
ÅTKOMST	12



INLEDNING OCH OMFATTNING

Inledning

Stadens övergripande regelverk omfattar all informationssäkerhet (bilaga 1) och styr verksamheternas IT-säkerhet. Stadens regler finns publicerade på intranätet och kan användas som uppslagsverk.

Denna instruktion är framtagen utifrån stadens övergripande regelverk för informationssäkerhet och vänder sig till all personal vid Norrmalms stadsdelsförvaltning som är IT-användare. Syftet med denna instruktion är att beskriva de regler och rutiner som gäller inom Norrmalms stadsdelsförvaltning. Instruktionen finns tillgänglig för alla användare på intranätet. Verksamhetsansvarig chef ansvarar för att personalen tagit del av och tillämpar instruktionen. Den reviderade instruktionen med bilagor har godkänts av Norrmalms stadsdelsnämnd 2007 –

Omfattning

Säkerhetsarbetet omfattar alla åtgärder vars samlade effekt är att förebygga och begränsa konsekvenserna av störningar för informationshantering inom våra verksamheter. Personer som omfattas är förtroendevalda, anställda och i viss omfattning skolelever samt konsulter/entreprenörer om uppdragens karaktär är relevanta för informationssäkerheten.

Klassificering av information

Informationstillgångar ska klassificeras (värderas) så att rätt skyddsnivå kan fastställas. Klassificeringen utgår från faktorerna Åtkomstbegränsning, Riktighet, Tillgänglighet och Spårbarhet.

IT-säkerhetssamordnaren kallar samman systemrepresentanter och systemförvaltare för en klassificering av respektive lokala system. Uppföljning sker minst vartannat år eller vid behov.

Kontinuitets- och avbrottsplanering

Stadsdelsförvaltningen har en övergripande kontinuitets- och avbrottsplanering (K/A plan) som omfattar åtgärder och prioriteringar. Verksamhetsansvariga chefer ansvarar för utformning och dokumentation av K/A planer som träder ikraft vid allvarligt och eller långvarigt datorbortfall i den egna verksamheten. Såväl reservrutiner som K/A planer ska 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. Ansvar för att hålla dessa rutiner aktuella åligger den verksamhetsansvarige chefen.

Säkerhetsuppföljning

Säkerhetsuppföljning utförs genom intern uppföljning med eller utan IT-stöd. Traditionell uppföljning eller attacksimulering kan även utföras av externa konsulter. Internrevision kommer att genomföras avseende t.ex. fillagring.

Förvaltningsledningen, IT-säkerhetssamordnaren eller IT-chefen är initiativtagare till säkerhetsuppföljningen.



IT-SÄKERHETSORGANISATION FÖR NORRMALM

IT-säkerheten är kopplad till det allmänna verksamhetsansvaret. Det betyder att varje chef som är ansvarig för en verksamhet i stadsdelen också är ansvarig för IT-säkerheten inom denna verksamhet.

Norrmalms stadsdelsnämnd

Norrmalms stadsdelsnämnd är ytterst ansvarig för IT-verksamheten inom sitt område och ska därför anta regler och anvisningar för IT-säkerheten. Med utgångspunkt från ovanstående har följande IT-säkerhetsorganisation utformats för Norrmalms stadsdelsnämnd.

Stadsdelsdirektör

Stadsdelsdirektören har det övergripande linjeansvaret för IT-säkerheten inom stadsdelsförvaltningen. Stadsdelsdirektören utser IT-säkerhetssamordnare, offentlighetsansvarig, kontaktperson mot datainspektionen, lokala systemförvaltare för egna system och förvaltningens systemrepresentanter för övergripande system. Stadsdelsdirektören är också ansvarig utgivare för stadsdelens publika sida på Internet.

Förvaltningens systemrepresentant för övergripande system

Systemrepresentanten svarar för att säkerhetsfunktionerna överensstämmer med fastställd skyddsnivå och ser till att sårbarhetsanalyser genomförs i samarbete med IT-säkerhetssamordnarna. Han genomför informationsklassning i samarbete med IT-säkerhetssamordnarna, samt kontrollerar att behörighetsadministrationen sköts för respektive system. Han bevakar att nödvändiga loggningsrutiner tillämpas och ser till att användarna får information om vilket skydd som gäller för systemet.

Förvaltningens systemrepresentanter förtecknas på sidan 7.

Systemförvaltare för lokala system

Systemförvaltaren ansvarar i enlighet med systemägarens anvisningar för systemets IT-säkerhet. Utsedda systemförvaltare för lokala system vid Norrmalms stadsdelsförvaltning förtecknas på sid. 7.

IT-säkerhetssamordnare

En IT-säkerhetssamordnare och en biträdande IT-säkerhetssamordnare utses av stadsdelsdirektören och ser till att nödvändiga riktlinjer utformas och beslutas för informationssäkerheten inom förvaltningen. Denne kontrollerar att övergripande regler och riktlinjer efterlevs inom förvaltningen, samt ansvarar för att sprida kunskap om regler, metoder och tekniker avseende IT-säkerhet. IT-säkerhetssamordnarna ansvarar för det gemensamma IT-säkerhetsarbetet.

IT-säkerhetssamordnaren är kontaktperson och rapporterar relevanta incidenter till stadens informationssäkerhetschef. IT-säkerhetssamordnare vid Norrmalms stadsdelsförvaltning är Barbro Broo och biträdande IT-säkerhetssamordnare, IT-chef Eva Eriksson.



IT-chef

IT-chefen samordnar det för stadsdelen gemensamma IT-arbetet och arbetet vid IT-enheten samt utformar och följer upp IT-strategiska frågor inom förvaltningen. IT-chefen ansvarar för driften av stadsdelsförvaltningens nätverk och installationer av datautrustning på avdelningar och enheter. Arbetet med att tilldela och kontrollera fysisk tillgång till utrustningen samt analyser av driftstörningar och efterföljande åtgärder ingår. IT-chef vid Norrmalms stadsdelsförvaltning är Eva Eriksson.

Allmänhetens kontaktperson

Kontaktpersonen håller aktuella förteckningar och beskrivningar över de IT-register som finns inom verksamheten och samordnar service mot de personer ur allmänheten som vill se offentlig information eller personinformation om sig själva. Här ligger även ansvaret för arkiv- och gallringsfunktionen. Respektive kontaktperson för olika register inom förvaltningen ska ansvara för framtagande av registerutdrag.

Till allmänhetens kontaktperson vid förvaltningen har utsetts arkivassistent, Håkan Nyland.

Verksamhetsansvarig chef (enhets- eller avdelningschef)

Verksamhetsansvarig chef ansvarar för att IT-säkerheten vid enheten eller avdelningen fungerar i enlighet med förvaltningens IT-säkerhetsinstruktion och ger behörighet till de verksamhetssystem han/hon ansvarar för. Se IT-säkerhetshandledning för chefer (bilaga 2).

Användare

Användarna ska följa fattade beslut avseende säkerheten i systemet. Användarna ska också rapportera funktions-störningar/fel i system, utrustning och data och övriga incidenter och händelser som kan äventyra säkerheten, till verksamhetsansvarig chef som i sin tur meddelar IT-säkerhetssamordnaren eller IT-enheten.

Användarnas ansvar specificeras ytterligare i den särskilda IT-säkerhetshandledningen för användare (bilaga 3). IT-säkerhetshandledningen finns tillgänglig för samtliga användare via stadsdelsförvaltningens intranät.

Projektledare

Projektledaren ska se till att verksamhetskraven på säkerhet fastställs och beaktas. Denne ska svara för att projektet bedrivs med de kvalitets- och säkerhetskontroller som stadgas i systemutvecklingsmodellen och övriga styrande dokument



Systemrepresentanter vid Norrmalms stadsdelsförvaltning

Ekonomisystem	Ekonomisk redovisning/uppföljning	Ekonomiavd
Lisa	Lön/PA	Ekonomiavd
Lisa Självservice	Administration	Ekonomiavd
Paraplyet	Äldreomsorg	Äldreomsorgen
Paraplyet	Handikappomsorg	Funktionshindre
Paraplyet	Iof	Sociala enheten
	Iof	Familjeenheten
	Iof	Socialpsykiatriska enheten
ParaSol	Dokumentation	Äldreomsorgen
VoDok	Dokumentation	MASen
Socialbidrag	Socialvårdsregister	Försörjningsstödsenh
BoSko	Barnomsorg, skolbarnomsorg	Barn- o Ungdomsavd
A70	Familjehemslöner	Ekonomiavd
J90	Behörighetssystem	IT-enheten
Bra	Behörighetssystem	IT-enheten
Diabas	Diarium	Planeringsavdelningen
Avgiftsnedsättning/ /KbH	Äldreomsorgen	

Systemförvaltare för lokala system vid Norrmalms stadsdelsförvaltning

HEP	Skuldsanering	Försörjningsstöd
Omsorg 2000	Individuell vårdplanering	Vård- och Omsorg

För information om vilken person som ansvarar för vilket system, kontakta IT-säkerhetssamordnaren eller IT-enheten.

Anvisningar för hantering av information vid sekretess

Det är väsentligt att varje anställd har kännedom om vilken information inom det egna ansvarsområdet som är sekretessbelagd och hur den skall hanteras. Prövning av sekretess föreligger för viss information varje gång begäran om utlämning av handling görs. Detta oavsett om handlingen är sekretessbelagd eller ej.

Respektive chef skall säkerställa korrekt hantering av sekretessbelagda handlingar. Tystnadsförbindelse skall tecknas med konsult/entreprenör som får ta del av sekretess-belagd handling.

Sekretessbelagda handlingar skall

- märkas med särskild stämpling/påteckning
- förvaras i säkerhetsskåp
- vid gallring förstöras i dokumentförstörare
- distribueras med bud eller rekommenderat brev med mottagningsbevis
- i elektronisk form, distribueras krypterade om teknisk plattform medger detta
- i elektronisk form, lagras krypterade om teknisk plattform medger detta



För sekretessbelagda handlingar som gäller rikets säkerhet enligt Sekretesslagen 2 kap, hänvisas till stadens säkerhetsskyddschef.

Material som lyder under sekretess ska aldrig publiceras på Internet eller på Intranätet.

Hantering av arbetsmaterial

Arbetsmaterial kan vara av olika slag. Ofta ingår arbetsmaterial i ett pågående ärende tillsammans med Allmänna handlingar. Det skall beaktas att det arbetsmaterial som dagligen hanteras kan resultera i en Allmän handling som kan efterfrågas för utlämnande.

Arbetsmaterial skall förvaras och distribueras på ett sådant sätt att full kontroll kan upprätthållas och informationen i arbetsskedet inte kan komma obehörig till hands. I samband med resor, konferenser och motsvarande skall arbetsmaterial hanteras på sådant sätt att exponering för obehöriga undviks.

Placering av utrustning

Utrustning där känslig information kan läsas (bildskärm, skrivare, fax) ska skyddas så att obehöriga inte kan ta del av informationen. Om fax skickas med känslig information bör kontakt tas med mottagaren innan faxet skickas.

Stöldskydd

All datorutrustning tillhörande Norrmalms stadsdelsförvaltning och är inköpt via IT-enheten stöldskyddsmärks. Lokaler där datorutrustning förvaras ska vara inbrottslarmade under icke arbetstid. I lokaler där utrustning förvaras på nedre botten ska fönstren vara larmade alternativt försedda med galler.

Finns risk för stöld kan t.ex. boxar övervägas om skalskydd eller miljö är sådan att stölder kan ske på ett enkelt sätt. Bärbara persondatorer bör vara försedda med wirelås för att förhindra stöld vid arbete i publik miljö.

Rutin för ID-uppvisande vid datorlån på Tulegatan 13 har upprättats för detta ändamål.

PERSONAL OCH SÄKERHET

Genom säkerhetsinsatser ska riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar. Målgruppen är, förutom anställda, i vissa fall även förtroendevalda och konsulter/entreprenörer.

Anställning

Uppgifter som lämnas i platsansökningar ska kunna verifieras och referenser ska tas i nödvändig omfattning. En kort information (bilaga 3) om den anställdes informationssäkerhetsansvar ska lämnas vid anställning av chefen vid respektive enhet/avdelning. Personal som kommer i kontakt med sekretessbelagda handlingar ska informeras om Sekretesslagen och dess innehåll. För viss verksamhet gäller fr.o.m. 2001-01-01 Lag om registerkontroll.



Vid nyanställning och upplägg av användarkonto i nätverket kommer den nyanställda att "kvittera ut" sitt användarkonto. Att "kvittera ut" innebär att den nyanställda ska ta del av stadsdelsnämndens dokument avseende IT-säkerhet med hantering av Internet och e-post. Därefter ska den nyanställda skriva på dokumentet och på så sätt bekräfta att han/hon förstått vad som gäller inom stadsdelen. Det påskrivna dokumentet arkiveras tillsammans med andra behörighetspapper i den nyanställdes mapp hos IT-enheten. Alla användare liksom konsulter och övriga tredjepartsanvändare, ska få anpassad och uppdaterad utbildning i vilka riktlinjer och rutiner som gäller vid förvaltningen.

Användardokumentation finns tillgänglig för användare på intranätet.

Tystnadsförbindelse ska upprättas för konsulter/entreprenörer med uppdrag inom stadsdelsförvaltningen.

Vid tjänstledighet > 6 månader samt för långtidssjukskrivna inaktiveras användarkontot. Se vidare Behörighetsrutinen. Vid övertalighet ska, om inte annat överenskommits, åtkomsträttigheter till system omgående avslutas.

Avslut/ändring av arbetsuppgifter

För de fall när personer slutar sin anställning eller övergår till annan enhet/andra arbetsuppgifter inom förvaltningen ska rutiner finnas som styr avveckling/förändring av tillgång till såväl lokaler som IT-system och information. Ansvar för detta ligger på den verksamhetsansvarige chefen.

Uppsägning/övertalighet

Användare med administratörsrättigheter eller högre behörighet till lokaler och system bör framtas dessa högre rättigheter/behörigheter omedelbart i samband med underrättelsen om förändringar. Normala användarbehörigheter kan behållas så länge personen är i tjänst. Möjlighet till riktad loggning ska beaktas.

Överträdelser

Överträdelser av förvaltningens IT-säkerhetsregler hanteras i första hand av verksamhetsansvarig chef och i andra hand av förvaltningsledningen. IT-säkerhetssamordnaren ska informeras för rapportering till stadens incidentrapporteringssystem, ISAP.

ANVÄNDARUTBILDNING

Verksamhetsansvarig chef ska se till att berörd personal ges möjlighet att genomgå utbildning i informationssäkerhet.

SÄKERHETSINCIDENTER OCH FUNKTIONSFEL

Incidentrapportering

Alla användare ska rapportera incidenter till verksamhetsansvarig chef som i sin tur



meddelar IT-säkerhetssamordnaren eller IT-enheten, vilka i sin tur rapporterar vidare till stadsdelsdirektören och till stadens incidentrapporteringssystem ISAP. Det kan gälla virusangrepp, intrångsförsök, felaktig hantering av personuppgifter, inbrott/inbrottsförsök eller funktionsfel som kan ha uppstått på grund av oegentligheter.



FYSISK SÄKERHET

Tillträdet till driftmiljön är reglerad. Passagekontroll via kodlås finns. Nycklar och passerkort hanteras av planeringsavdelningen. Vid externa besök följer behörig personal med. Stadsdelen har en publik dator som är placerad inom det yttre skalskyddet i receptionen på Tulegatan 13.

BÄRBARA DATORER

Bärbara datorer/handdatorer ska stöldskyddsmärkas och krypteras vid behov. Datorerna ska installeras med antivirusskydd. Om den bärbara datorn är uppkopplad till nätverket sker detta med automatik.

Uppringd kommunikation sker enligt stadens standard via modem, ISDN eller ADSL och inloggning via engångslösenord eller stadens ID-portal.

Om brister upptäcks i säkerheten t.ex. att krypteringsskydd saknas eller om regler/rutiner saknas för något moment ska den närmaste verksamhetschefen informeras som i sin tur meddelar IT-säkerhetssamordnaren eller IT-enheten. Stölder av bärbara datorer ska polisanmälas och rapporteras till IT-enheten. Förvaltningens regler för E-post och Internet gäller även vid användande av bärbara datorer.

Användandet av bärbara datorer skapar frihet och flexibilitet i arbetet och det är varje användares skyldighet att följa de regler som gäller inom förvaltningen. Bärbara datorer och de datorer som inte är anslutna till nätverket och som hanterar känslig information ska ha filkrypteringsskydd på hårddisken.

Förvaring av bärbara datorer

Den bärbara datorn ska förvaras på ett säkert sätt vid exempelvis konferenser, i bilen, på resor och i den egna bostaden.

Säkerhetskopiering

Information som finns lagrad på den bärbara datorn ska säkerhetskopieras. Det är användarens ansvar att så sker. Tänk på att inte förvara säkerhetskopierna tillsammans med datorn.

DISTANSARBETE

Samma säkerhetsnivå gäller för distansarbetsplats som för ordinarie arbetsplats.

ARBETE UTANFÖR DEN EGNA ARBETSPLATSEN

Vid arbete med känsliga personuppgifter eller förvaltningsintern information utanför den egna arbetsplatsen, ska datorn vara placerad så att ingen utomstående kan se vad som skrivs. Lämna inte datorn utan uppsikt.



KOMMUNIKATION

Datakommunikation

I samband med att information överförs genom datakommunikation uppkommer risker för avlyssning eller förändring av den överförda informationen. Behov av skydd för röst-, fax- och videokommunikation ska beaktas.

Modem

Modem får ALDRIG kopplas till en persondator som är ansluten till stadsdelens nät. All extern kommunikation ska ske via stadens gemensamma modempool.

Fjärråtkomst

All uppringd analog kommunikation ska ske med hjälp av engångslösenord, som genereras för varje tillfälle eller stadens ID-portal. ISDN/ADSL-kommunikation ska ske med hjälp av krypterat lösenords utbyte mellan routrar.

Dokumentation

För lokala system ligger dokumentationsansvaret på lokal systemägare/förvaltare.

LOGGHANTERING

Stadsdelen är pilotförvaltning avseende loggshantering. En programvara för ändamålet kommer att installeras och transaktionsloggar kommer att skapas för de administratörer som har tillgång till systemen. Transaktionsloggning utförs på lokala-, centrala- och externa administratörer. Tillgång till och genomgång av loggarna kommer stadsdelens IT-säkerhetssamordnare att ha.

SÄKERHETSKOPIERING

Varje dygn tas en säkerhetskopia över förändringar som skett i förvaltningens nätverk. Det innebär att såväl programvaror som information kopieras. En fullständig säkerhetskopia tas varje vecka respektive månad. Vecko- och månadskopiorna sparas åtskilda som säkerhetskopior. Återläsning testas med jämna mellanrum.

Om information lagrats på persondatorns hårddisk ansvarar respektive användare själv för säkerhetskopiering.

DATAVIRUS OCH SKADLIGA PROGRAM

Skydd mot skadliga program

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.



Endast program godkända av förvaltningen får användas. Antivirusprogram installeras och uppdateras kontinuerligt på samtliga nätanslutna datorer på förvaltningen. IT-enheten kan hjälpa till vid frågor om detta. Privata program och spel får varken installeras eller användas.

STYRNING AV NÄTVERK

Åtkomst

Åtkomsten till nätverket och de olika systemen styrs genom behörigheter och rättigheter. Verksamhetsansvarig chef beställer behörighet för respektive anställd. Behörigheten läggs upp av IT-enheten och beställningsformuläret sparas i respektive användares mapp hos IT-enheten.