S

IT-säkerhetshandledning för användare

Norrmalms stadsdelsnämnd har 2003…… fastställt en reviderad IT-säkerhetsinstruktion för nämndens verksamhet. Instruktionen skall finnas tillgänglig för alla användare.

Varje användare har ansvar för att för sin egen del följa de instruktioner som gäller för IT-säkerheten. Som ett stöd i detta har denna handledning utarbetats. Den gör inte anspråk på att vara heltäckande men bör fungera som en lathund i det dagliga arbetet.

Allmänt

☞ Om du upptäcker brister i säkerheten eller saknar regler/rutiner för något moment är du skyldig att informera din chef , som i sin tur meddelar IT-säkerhetssamordnaren.

Behörighet och lösenord

☞ Du har som användare tilldelats den behörighet till olika system och program krävs för att du ska kunna sköta dina arbetsuppgifter. Ansvarig för till delning av behörigheter är närmast verksamhetsansvarig chef (enhetschef eller avdelningschef).

☞ Behörighet tilldelas i form av ett användar-ID och ett hemligt lösenord. Behörigheten är personlig och får inte överlåtas på annan, inte ens tillfälligt.

☞ Lösenordet är hemligt. Om du misstänker att någon fått reda på ditt lösenord måste du omgående byta. Lösenordet skall vara individuellt och får inte överlåtas eller lånas ut. Lösenordsbyte krävs automatiskt var 30:e dag.
Ditt lösenord måste vara sammanhängande, minst 6 tecken och maximalt 8 tecken långt. Lösenordet ska bestå av en blandning av alfa-numeriska tecken, men inte bokstäverna åÅ, äÄ, och öÖ eller vissa specialtecken som t.ex. @, }, %, £
Repeterbarhet av lösenord är förhindrat i 13 ”generationer”.
I de flesta fall görs intrång i datasystem genom att lösenord avslöjats på något sätt. Tänk därför på följande:
Välj ett lösenord som är svårt för andra att gissa. Använd ej namn på familjemedlemmar, telefonnummer, bilnummer och liknande.
Kombinera siffror och bokstäver.
När du byter lösenord, får du inte använda system av typen Tule1 ändras till Tule2 o.s.v.

Undvik att skriva upp lösenord, men om du gör det så använd en ”personlig kryptering” och förvara lappen på ett säkert ställe (inte under musmattan eller skrivbordsunderlägget).

☞ Din PC är utrustad med skärmsläckare med lösenordsfunktion. För användare anslutna till nätverket startar skärmsläckaren efter 10 minuter. Övriga användare, som ej är anslutna till nätverket, skall aktivera skärmsläckaren och lösenordsfunktionen.

☞ Lämna aldrig din PC obevakad när du har loggat på med ditt lösenord. Se till att skärmsläckaren med lösenord släckt bildskärmen när du lämnar din arbetsplats (Ctrl + Alt + Del).

☞ Om du har glömt ditt lösenord eller ”kastats ut” efter tre felaktiga inloggningsförsök, tag kontakt med IT-enheten så hjälper de dig (tel. 508 09 010). Om det gäller ett stordatorsystem ska du ringa till TIETO ENATORS helpdesk (tel. 83 83 00).

☞ Avsluta alla program och stäng av din PC (=logga ur) innan du går hem för dagen.

Lagring av information

☞ Om du är ansluten till nätverket skall lagring av information i första hand ske på servern. Detta ger större säkerhet eftersom backuper sker regelbundet centralt och servern har åtkomstskydd genom nätets behörighetskontrollsystem. Lagring av data på hårddisken (C:) eller på diskett (a:) bör inte ske eftersom åtkomstskyddet för information som lagras på detta sätt är sämre.

☞ Om du av olika skäl ändå måste lagra information på hårddisken (t.ex. om du inte är ansluten till nätverket) svarar du själv för säkerhetskopiering. Hur ofta du skall säkerhetskopiera beror på hur ofta den information som finns lagrad i datorn förändras. Säkerhetskopior skall förvaras väl skyddade mot stöld, skada , brand, damm, smuts m.m. Rådgör alltid med IT-enheten om du är osäker.

☞ Om du lagrar information på diskett svarar du för att disketten inte förvaras i direkt anslutning till datorn. Disketter med viktig eller känslig information skall förvaras i brandsäkert säkerhetsskåp. Övriga disketter kan förvaras i skåp eller skrivbordslåda i arbetsrummet.

Datavirus

☞ All data och e-post som lagras på servern virus-scannas automatiskt. Lokala Hårddiskar och disketter scannas av användaren. Datorer som ej är anslutna till nätverket skall vara utrustade med programvara för virustest. Rådgör alltid med IT-enheten om du är osäker på hur du ska gå tillväga.

☞ Du bör inte kopiera filer och ska inte kopiera program från Internet då det innebär en ökad risk för virussmitta. Rådgör alltid med IT-enheten om du ändå behöver kopiera filer eller program från Internet.

☞ Privata program och spel får inte användas. Endast program godkända av förvaltningen får användas. Rådgör med IT-enheten om du är osäker.

Hantering av utdata

☞ Du ansvarar för att listor och dokument som du skriver ut och som är av känslig karaktär förvaras så att de inte kan läsas eller kopieras av någon obehörig.

☞ Du ansvarar för att listor och dokument som är av känslig karaktär och som skickas till dig, via post, fax, e-post eller på annat sätt, hanteras på ett riktigt sätt.

Integritetskänslig/sekretessbelagd data

Utöver vad som ovan angivits under allmänt gäller följande

☞ Du bör inte arbeta med integritetskänslig/sekretessbelagd data på bärbara PC:n.

☞ Du bör inte lagra integritetskänslig/sekretessbelagd data på diskett. Om så sker får disketten inte lämnas obevakad under arbetets gång. Förvaring av disketten skall ske i IT-säkerhetsskåp.

☞ Vid utskrift av integritetskänslig/sekretessbelagd data måste du bevaka utskriften så att datan inte kommer till andras kännedom.

☞ Integritetskänslig/sekretessbelagd information lagrad på server/hårddisk/diskett ska utplånas så fort som den inte längre behövs.

☞ Utplåning ska ske så att uppgifterna inte kan återskapas. Det innebär att utplåning ska ske genom överskrivning. Rådgör med IT-enheten vid frågor om detta.