AE NORRMALMS STADSDELSFÖRVALTNING

PERSONALAVDELNINGEN

TJÄNSTEUTLÅTANDE

DNR 054-934/02

Handläggare: Barbro Broo, tel 08-508 09 049

Till
Norrmalms Stadsdelsnämnd

Kontinuitets- och Avbrottsplan gällande IT-stödd verksamhet

Förslag till beslut

Kontinuitets- och avbrottsplan gällande IT-stödd verksamhet för Norrmalms stadsdelsförvaltning godkänns.

Ylva Tengblad
stadsdelsdirektör

Lars B. Strand
t.f. avdelningschef
Strategi- och stöd

Sammanfattning
Dagens behov av IT-stöd i verksamheterna medför ökade konsekvenser i och med att riskerna för avbrott i informationsbehandlingen växer.
Olika driftsavbrott kan inträffa som kan medföra allt ifrån försumbara konsekvenser till avbrott som ger katastrofala konsekvenser för verksamheten.
Förvaltningar och bolag skall i enlighet med de IT-säkerhetsregler som Stockholms stad antagit upprätta kontinuitets- och avbrottsplaner för IT-stödd verksamhet.

Ärendets beredning
Ärendet har utarbetats vid Personalavdelningen i samarbete med Strategi- och stödavdelningen. Förslag till tjänsteutlåtandet har behandlats i Förvaltningsgruppen den 2002-12-06

Bakgrund
Varje förvaltning m fl skall enligt de IT-säkerhetsregler som gäller i staden upprätta Kontinuitets- och avbrottsplaner för IT-stödd verksamhet.

Förvaltningens förslag
Med kontinuitets- och avbrottsplanering avses planering av åtgärder mot störningar som är så svåra att de inte kan bemästras inom ramen för de normala rutinerna och resurserna. De ekonomiska konsekvenserna kan vara av så stor betydelse att verksamheten äventyras.
Med anledning av detta erfordras reservsystem och rutiner för återställande. Avbrottsrutiner kan innebära, dels manuella rutiner, dels starkt reducerade IT-rutiner eller en kombination därav.

Ansvar och befogenheter
Förvaltningsledningen är ytterst ansvarig för den totala IT-säkerheten dvs mål och riktlinjer efterlevs.

Varje chef är ansvarig inom sin verksamhet för att:
- Identifiera och klassificera den information som hanteras inom verksamheten
- Införa och upprätthålla fastställda regler för säkerhet och skydd för IT (förvaltningens reviderade IT-säkerhetsinstruktion)
- Förvissa sig om att berörda medarbetare är informerade och förstår sitt ansvar när det gäller säkerheten och skydd för IT
- Identifiera och värdera risker när det gäller IT-säkerheten
- Rapportera risker och incidenter till IT-enheten eller IT-säkerhetssamordnarna, vilka i sin tur rapporterar till stadsdelsdirektören och till stadens IT/informationssäkerhetschef

Varje berörd anställd har ett ansvar för att:
- Följa arbetsplatsens och förvaltningens reviderade IT-säkerhetsinstruktion
- Rapportera risker och incidenter till närmaste chef, IT-enheten eller IT-samordnarna. Exempel på incidenter som skall rapporteras är: virusangrepp/virusindikation, intrångsförsök, felaktig hantering av personuppgifter, inbrott/inbrottsförsök, eller funktionsfel som kan ha uppstått pga oegentligheter

- Ta väl vara på information som i orätta händer kan skada verksamheten/förvaltningen i helhet

Organisation:
Organisationen vid ett driftstopp ska följa stadsdelsförvaltningens ordinarie linjeorganisation i möjligaste mån. I de fall detta inte är möjligt, exempelvis vid ett större driftstopp träder delar av förvaltningens katastroforganisation in.

Övergripande åtgärder vid ett avbrott

- Stadsdelsdirektören samråder med avdelningschefen för Strategi- och stöd om avbrottets storlek och omfattning.
  En ledningsgrupp utses, vars uppgift är att svara för beslut om vilka åtgärder som ska initieras, samt för planering, ledning, samordning och uppföljning under den uppkomna situationen.

- Stadsdelsdirektören alternativt avdelningschefen för strategi- och stöd, beroende på omfattningen av driftsstoppet, sammankallar berörda i ledningsgruppen till ett första möte.
  Berörda i detta första skede kan vara: IT-säkerhetssamordnarna, informatören, samt personal från IT-enheten. Genomgång görs av vilka verksamheter som berörs.
  Inventering görs av antal bärbara datorer och övriga användbara datorer som finns tillgängliga på förvaltningen.
  Finns möjlighet att arbeta i en annan lokal på förvaltningen, alternativt annan stadsdelsförvaltning.
  Kontakt tas vid behov med annan förvaltning.

- Informationsansvarig för intern och extern information utses.
  Informera växeln på Tulegatan 13.

- Möte hålls med berörda verksamheters chefer.
  Prioritering görs av arbetsuppgifter och funktioner.

- Stadsdelsdirektör alternativt avdelningschefen för strategi och stöd beslutar om vilka reservrutiner som är aktuella.
  Beslut tas av stadsdelsdirektören om övergång till reservrutiner och eventuell katastroforganisation.

- Informationsansvarig tar tillsammans med IT-säkerhetssamordnarna fram information till drabbade användare, massmedia och brukare.

Det är viktigt att snabb information om vad som har hänt och hur länge avbrottet beräknas pågå ges till berörda enheter/ användare så att dessa ges möjlighet att planera sina arbetsinsatser.

- Kontinuerliga möten i ledningsgruppen hålls under avbrottet/störningen.

- Allt eftersom IT-resurserna börjar fungera igen, återuppbyggs verksamheterna enligt uppgjord prioritetsordning

- Stadsdelsdirektör beslutar om avveckling av reservrutiner/katastroforganisation och återgång till normalrutiner.

- IT-säkerhetssamordnarna genomför en analys av störningen alternativt avbrottet. Analysen bör innehålla uppgifter om orsaker till störningen/avbrottet, omfattning och konsekvenser. Erfarenheterna ska dokumenteras skriftligen.

Uppföljning av rutiner efter avbrottet
Det är viktigt att berörd chef följer upp rutinerna efter ett avbrott och skriver en avvikelserapport.
Följande frågor bör besvaras:
- ge en beskrivning av händelseförloppet
- hur länge och vid vilken tidpunkt inträffade avbrottet
- vilka reservrutiner användes och hur fungerade de
- behövs rutinerna förbättras/ändras och på vilket sätt iså fall

Rapporten lämnas till IT-säkerhetssamordnarna senast tre veckor efter avbrottet.

Översyn och kontroll
Respektive ansvarig chef för verksamheten skall tillse att antagna reservrutiner uppdateras och i övrigt hålls levande genom övningar och tester.
Berörd personal skall informeras om antagna reservrutiner.
Det är viktigt att personalen känner till sina uppgifter vid ett avbrott och att nödvändiga förberedelser genomförts.
Översyn av Kontinuitets- och avbrottsplanen skall ske kontinuerligt och anpassas till inträffade eller planerade förändringar.
Tester av avbrottsplanen skall dokumenteras. Det är viktigt att de eventuella brister som upptäcks dokumenteras, i syfte att åtgärdas vid en revidering av avbrottsplanen.

Obehörigt tillträde/åtkomst till information och lokaler:

Vid upptäckt av obehörigt tillträde till lokaler och arbetsrum, skall detta snarast rapporteras till närmaste chef, detta gäller även när utrustning, information eller om något annat försvunnit från arbetsrum eller lokaler.

Vid upptäckt av obehörigt tillträde till datorer/information eller nätverk skall detta snarast rapporteras till närmaste chef, IT-enheten eller IT-säkerhetssamordnarna.
Det är viktigt att ingen rör utrustningen efter upptäckt, då viktig information för spårbarhet annars kan gå förlorad.

I båda fallen avvakta till dess IT-enhetens personal och/eller polis undersökt händelsen.

Larm om virus incident:

- namn på virus
- hur sprider det sig
- vad gjorde personen när viruset hittades
- vilken dator, sökväg, filnamn och anti-virusprogram används (vilken version), varifrån kommer filen
- vem hittade viruset och när
- har viruset hittats i ett dokument som tidigare använts internt, i utgående e-post eller inkommande e-post