Dnr

RIKTLINJER

Riktlinjer för IT-resurser inom Nyköpings kommun

Antagen av

Nyköping
www.nykoping.se

Innehållsförteckning

Inledning

Detta dokument beskriver de riktlinjer som gäller för hantering av digital information och informationsbärare i form av datorer, mobiltelefoner och externa minnen etcetera samt drift och förvaltning av kommunens IT-resurs.

Riktlinjer för att ansvar för kommunens samlade IT-resurser blir tydligt fastställs av kommundirektören i samråd med centrala ledningslaget.

Riktlinjerna reglerar:

- ansvar för infrastruktur för kommunikation och ägande av all IT-utrustning
- det totala ansvaret för centrala system och för IT-arkitektur i kommunens IT-miljö
- ansvar för att systemen i kommunen konsolideras, standardiseras och samordnas inom divisionerna och de centrala enheterna
- ansvar för att ett aktivt arbete med IT-säkerhet och riskanalys bedrivs
- ansvar för verksamhetsspecifika system

Riktlinjen gäller tillsvidare.

1 Mål

Informationssäkerhet ska utgå från att Nyköpings kommun även fortsättningsvis ska utgöra en öppen miljö där verksamheter och enheter har stora möjligheter att utforma sitt egna IT-stöd. Med kännedom om den ständigt förändrade hotbilden mot system och information är det nödvändigt att vidta IT-säkerhetsåtgärder som i vissa fall kan komma att inskränka öppenheten.

Arbete med IT-säkerhet och riskanalys ska ske aktivt för att Nyköpings kommuns verksamheter effektivt och med hög säkerhet ska kunna utföra sin uppgift att ge service till kommuninvånarna.

Informationssäkerhet ska ha som mål att anställda, förtroendevalda och elever ska kunna använda IT-resurser utan oönskade störningar och med hög grad av:

- tillgänglighet
- tillförlitlighet
- spårbarhet
- sekretess

IT-resurserna i kommunen ska användas på ett effektivt sätt så att största möjliga nytta ska uppnås. Detta ska ske genom att systemen i kommunen konsolideras, standardiseras och samordnas inom och mellan divisionerna och de centrala enheterna.

2 Riktlinjer för informationssäkerhet

2.1 Definitioner

I de dokument som reglerar informationssäkerhet inom kommunen används följande begrepp:

Sekretess: Att information inte görs tillgänglig eller avslöjas för obehöriga.

Riktighet: Att information inte kan förändras obehörigen, av misstag eller på grund av funktionsstörning.

Tillgänglighet: Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid.

Spårbarhet: Att ändringar och åtkomst är spårbar i informationssystemen.

Tillgång: Allt som är av värde för kommunen: information, IT-utrustning, programvaror etcetera

Incident: En möjlig oönskad händelse som kan vara avsiktlig eller oavsiktlig.

Extraordinär händelse: En mycket allvarlig händelse där tillgängliga resurser är otillräckliga i förhållande till det akuta behovet och belastningen är så hög att normala kvalitetskrav, trots adekvata åtgärder, inte längre kan upprätthållas.

2.2 Hantering av utomstående parter

Syfte: Att säkerställa att nivån på informationssäkerheten är densamma oavsett om informationsbehandlingen sker med interna resurser, externa anordnare, externa leverantörer eller inhyrda konsulter.

All användning av konsulter, externa leverantörer och externa utförare ska regleras genom avtal. Dessa ska ha kännedom om Nyköpings kommuns informationssäkerhetspolicy och riktlinjer samt följa dessa.

Konsulter, externa leverantörer och externa utförare som kan komma i kontakt med sekretesskyddad information ska underteckna en sekretessförbindelse samt vara behöriga att ta del av informationen.

Det är inte tillåtet som konsult att ta med sig egen datorutrustning, använda den eller sammankoppla den med Nyköpings kommuns övriga utrustning, om detta inte har godkänts av IT-enheten.

För externa utförare gäller fastställd rutin för uppkoppling till verksamhetssystem.

Ansvar

Systemägare
Respektive systemägare har inom sitt ansvarsområde ett ansvar för att all personal, konsulter, externa leverantörer och externa utförare, har fått tillräcklig information och utbildning i säkerhet och i de informationssystem som de använder.

Systemansvarig
Systemansvarig som beställer tjänster av utomstående leverantörer ska följa upp och granska att säkerhetsöverenskommelser följs.

Relaterade rutiner

Rutin, avtal för konsulter, externa leverantörer och externa utförare inklusive sekretess-förbindelse.

Rutin, koppla in en dator, som inte ägs av Nyköpings kommun, i Nyköpings kommuns nätverk.

Rutin, åtkomst för externa utförare till verksamhetssystem.

2.3 Informationsklassning

Syfte: Att säkerställa att informationstillgångar får en lämplig skyddsnivå.

All information som lagras elektroniskt, med vissa undantag, i en kommun är att betrakta som allmän handling. Först vid begäran av utlämning av handlingen sker sekretessprövning enligt gängse lagkrav.

Vissa handlingar är sekretesskyddade i enlighet med Sekretesslagen.

Ansvar

Den person som skapar information (informationsägaren) ansvarar för att information hanteras i enlighet med gällande regelverk och nationell lagstiftning.

Relaterad rutin

Förvaltade verksamhetssystem och program

2.4 Hantering av informationstillgångar

Syfte: Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

Med datamedia menas CD-skivor, USB-minnen etcetera. Dessa medier ska inte ses som slutliga förvaringsformer såvida de inte avser backuptagning. Information på datamedia är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess beaktas. De krav på sekretess (tillgänglighet och riktighet) som ställs för ett specifikt IT-system framgår av den informationsklassning som löpande genomförs och är kända av systemförvaltaren samt IT-enheten.

För information på datamedia gäller följande krav:

Krav på sekretess	Åtgärder
Sekretesskyddad	**Förvaring** Vid lagring på bärbar dator och dylikt ska godkänd kryptering användas. CD-skivor, USB-minnen och dylikt som används ska förvaras säkert så att de ej är tillgängliga för obehöriga. **Kopiering** Kopiering får endast ske efter godkännande av systemägaren. **Spridning** Får flyttas fysiskt efter samråd med systemägaren om lämpligt

	tillvägagångssätt. Får endast distribueras till behöriga. Informationen ska hållas inom ett begränsat antal individer. **Återanvändning** Får inte användas för information klassad som intern eller öppen utan att först ha överskrivits med programvaran Wipe eller motsvarande för säker filradering. **Makulering** Lämnas till IT-enheten för förstöring.
Intern	**Förvaring** Vid lagring på bärbar dator och dylikt ska godkänd kryptering användas. De CD-skivor, USB-minnen och dylikt som används ska förvaras säkert så att de inte är tillgängliga för obehöriga. **Kopiering** Får kopieras i samråd med systemägare. **Spridning** Får endast distribueras till behöriga läsare. **Återanvändning** Får användas för information som är klassad intern eller öppen. **Makulering** Lämnas till IT-enheten för förstöring.
Offentlig	**Förvaring** Inga krav. **Kopiering** Tillåten. **Spridning** Tillåten. **Återanvändning** Får användas för information som är klassad intern eller öppen. **Makulering** Krävs ej.

2.5 Personal och säkerhet

Syfte: Att säkerställa att anställda, förtroendevalda, leverantörer och utomstående användare är medvetna om hot och problem som rör informationssäkerhet, sitt ansvar och sina skyldigheter. Målsättningen är att minska risken för mänskliga fel.

Information och utbildning av anställda ska omfatta:

- informationssäkerhetens betydelse för verksamheten
- innehållet i informationssäkerhetspolicyn

Nya användare ska ges en grundläggande utbildning, samt ges information om gällande regelverk kring informationssäkerhet före tilldelning av behörighet i nätverket.

Ansvar

Respektive chef
Alla chefer ansvarar för att de anställda inom organisationen eller avdelningen har rätt kunskap och nödvändig information om informationssäkerhet.

IT-enheten
IT-enheten tillhandahåller en grundutbildning om informationssäkerhet.

Anställd
Alla anställda och förtroendevalda ansvarar för att ta del av den utbildning som erbjuds samt de dokument som finns inom Nyköpings kommun för att reglera informationssäkerheten. De anställda och förtroendevalda ska följa det regelverk som finns inom kommunen.

Relaterad rutin

Rutin om internutbildningens frekvens och innehåll.

2.6 Anställning och avgång

Syfte: Att säkerställa att anställda och förtroendevalda är införstådda med sitt ansvar och den roll som de avser att ha, och på så sätt minska risken för stöld, bedrägeri eller missbruk av resurser. För att säkerställa att anställda och förtroendevalda lämnar organisationen, eller ändrar sina anställningsförhållanden, på ett ordnat sätt.

Vid anställningens början ansvarar den nyanställde att:

- ta del av den utbildning som ges kring informationssäkerhet
- ta del av, samt följa det regelverk (informationssäkerhetspolicy, riktlinjer samt rutiner) som finns kring informationssäkerhet

Vid speciella tjänster bör adekvat bakgrundskontroll göras.

När anställningen upphör ska den som slutar rådgöra med närmaste chef om vilket arbetsmaterial som ska sparas. Notera att allt arbetsmaterial som har framställts anses vara Nyköpings kommuns egendom och får inte tas med utan chefs godkännande.

De behörigheter som har erhållits för åtkomst till kommunens informationssystem ska avbeställas av närmaste chef. Material som inte är relevant för Nyköpings kommuns framtida verksamhet ska tas bort.

Ansvar

Respektive chef
Samtliga chefer ansvarar för att ge och revidera åtkomst till system för de anställda inom organisationen eller avdelningen.

IT-enheten
IT-enheten tillhandahåller underlag för revision i enligt med instruktion från systemägare.

Anställd
Alla anställda ansvarar för att ta del av den utbildning som erbjuds samt de dokument som finns inom Nyköpings kommun för att reglera informationssäkerheten. De anställda ska följa det regelverk som finns inom kommunen.

Relaterad rutin

Rutin att beställa och skapa en ny användare vid nyanställning.

Rutin att hantera användare och användarkonton vid förändrade anställningsförhållanden.

Rutin att hantera användare och användarkonton vid avsked.

2.7 Elektronisk lagring av information

Syfte: Att säkerställa att anställda, förtroendevalda och leverantörer använder utrustning och information på ett sådant sätt att en hög informationssäkerhet bibehålls.

Den information som lagras på Nyköpings kommuns gemensamma utrymmen säkerhetskopieras automatiskt. Den kan lagras på anvisade enheter.

Information som är lagrad på en dators lokala hårddisk kan utan några större resurser bli tillgänglig för obehöriga. Om sekretesskyddad information måste lagras på en bärbar dator eller en dator som används för distansarbete ska datorn ha ett rimligt skydd mot stöld samt krypterad hårddisk. När information lagras på lokal hårddisk är användaren personligen ansvarig för säkerhetskopiering. Den information som finns på en lokal hårddisk riskerar att förloras om den inte kan återskapas till rimliga kostnader vid till exempel en diskkrasch. Undvik därför, både av sekretesskäl samt säkerhetskopierings skäl, att lagra information på datorns lokala hårddisk.

Om Nyköpings kommuns datorer används för distansarbete ska det beaktas att den kan utgöra en säkerhetsrisk. Det får därför inte lagras sekretesskyddad information lokalt såvida inte hårddisken har godkänd kryptering.

Den anställde ska inte lagra privat material i kommunens IT-system.

Gallring av personligt lagringsutrymme

För utförlig information om gallringsfrist, se dokumenthanteringsplan IT-enheten på IN.

Ansvar

IT-enheten
IT-enheten har ansvar för att backup genomförs på filservrar och att dessa backuper hanteras samt förvaras på ett säkert sätt.

Anställd
Alla anställda ansvarar för att lagra den information de hanterar inom tjänsten så att sekretessen, tillgängligheten samt riktigheten inte äventyras. Det innebär att information ska lagras på kommunens centrala lagringsutrymmen.

2.7.1 Relaterad rutin

Rutin för att kryptera filer.

Rutin för distansarbete.

Rutin över backup.

2.8 Etiska regler

Syfte: Säkerställa att användarnas agerande på såväl internt nätverk som Internet inte ökar Nyköpings kommuns riskexponering.

När anställda och förtroendevalda använder Internet kan säkerheten i Nyköpings kommuns lokala nätverk påverkas i mycket hög grad.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande eller har anknytning till kriminell verksamhet.

I specifika fall kan det dock vara motiverat för arbetet, till exempel vid utredningar, omvärldsanalyser med mera, att besöka sidor som normalt är förbjudna. Beslut om detta ska fattas av närmaste chef.

Tänk på att när du surfar på Internet representerar du Nyköpings kommun och lämnar spår efter dig i form av Nyköpings kommuns IP-adresser. All användning av intranät eller Internet via Nyköpings kommuns internetuppkoppling är spårbar i loggar som finns tillgängliga för IT-enheten i den händelse att det finns behov av utredning av brott eller missbruk.

Sabotage eller störande verksamhet mot system eller andra användare samt intrång eller försök till intrång i system, lokalt såväl som på system utanför Nyköpings kommun, är förbjudet.

Installation av programvaror får endast ske av eller i samråd med IT-enheten. Samtliga programvaror som är installerade i Nyköpings kommuns IT-miljö ska vara licensierade och inköpta av Nyköpings kommun. Att installera eller använda piratkopierade produkter på datorerna är inte tillåtet. Det är inte heller tillåtet att kopiera programvara som är inköpt av Nyköpings kommun.

Ansvar

Verksamhetsansvarig chef
Verksamhetsansvarig chef ska godkänna om anställd behöver använda material på ett sätt som kan uppfattas som diskriminerande eller kriminellt. Användningen måste vara tjänsterelaterad och godkännandet ska dokumenteras och signeras i förhand.

IT-enheten
IT-enheten ska tillgodose verksamheten och systemens spårbarhetskrav. Vid behov ska analystjänster tillhandahållas.

Anställd
Alla anställda ska följa Nyköpings kommuns etiska regler och använda Internet utan att riskera att Nyköpings kommuns rykte påverkas negativt. All användning av datorer och nätverk ska ske utan att lagar eller Nyköpings kommuns interna regler överträds. Användning får inte heller förknippas med något brottsligt och orsaka Nyköpings kommun ekonomisk förlust.

2.9 Fysisk säkerhet

Syfte: Att förhindra obehörigt fysiskt tillträde, skador och störningar i IT-enhetens lokaler och information.

Ett bra fysiskt skydd av IT-enhetens lokaler och utrustning ska uppfyllas. Därför ska lokaler förses med inbrottsskydd och brandskydd i den omfattning som krävs.

All kritisk och känslig utrustning ska ges ett särskilt fysiskt skydd mot obehörigt tillträde samt skyddas mot brand, luftföroreningar, olämpliga klimatförändringar och vattenskador.

Tillträdesregler för säkra utrymmen, röd zon

Datorhallar som har resurser och informationssystem med känslig information ska vara försedda med kontrollsystem för in- och utpassering. Utrymmen med konsolutrustning och kopplingspunkter ska vara låsta när de är obemannade.

Om servicepersonal etcetera ges tillträde till säkrade utrymmen ska övervakning av personens arbete ske. Beslut ska tas av IT-chefen ifall sådant tillträde ska godkännas.

Ansvar

IT-chef
IT-chefen ansvarar för att de anställda har rätt behörighet på sina inpasseringskort samt att utrustning är skyddad i enlighet med riktlinjerna.

Anställd
Alla anställda på IT-enheten ansvarar för att de besökare som tas emot registreras samt att de aldrig lämnas utan sällskap. Alla anställda på IT-enheten ska bära sitt eget ID-kort synligt.

Relaterad rutin

Rutin för att ta emot externa besökare.

Rutin vid inbrottslarm och brandlarm.

2.10 Elektronisk kommunikation

Syfte: Att erhålla en hög informationssäkerhet för information som skickas elektroniskt internt eller externt.

Informationens klassning ställer alltid kravet på dess distributionsform.

Systemintegration

System som använder en extern part för informationsutbyte ska innan produktionssättning föregås av en riskanalys och utifrån dess resultat säkerställa att rätt kommunikationsmetod används.

E-post

E-post ska hanteras så att Nyköpings kommun inte bryter mot offentlighetsprincipen eller andra lagar och regler. Det ska också säkerställas att sekretessbelagd information inte distribueras via e-post.

Sociala medier

Sociala medier ska hanteras så att Nyköpings kommun inte bryter mot offentlighetsprincipen eller andra lagar och regler. Det ska också säkerställas att sekretessbelagd information inte distribueras via sociala medier.

Ansvar

Respektive chef
Samtliga chefer ansvarar för att alla anställda inom den egna enheten eller ansvarsområdet har tillgång till, samt kännedom om, riktlinjer för hantering av elektronisk kommunikation.

IT-enheten
IT-enheten ansvarar för att system för elektronisk kommunikation är konfigurerade så att informationssäkerhet uppnås.

Anställd
Alla anställda ansvarar för att ta del av dessa riktlinjer samt följa dem.

Relaterad rutin

Rutiner för användning av sociala medier.

2.11 Övervakning och loggar

Syfte: Att upptäcka obehörig informationsbehandling, ha spårbarhet av händelser samt identifiera problem med informationssystemen.

Säkerhetsrelevanta händelser ska loggas i den omfattning och detaljeringsgrad som verksamheten kräver, så att följderna av en attack mot systemet eller informationen kan spåras och begränsas. Loggningen har även en förebyggande effekt genom att avskräcka från obehöriga aktiviteter. Loggarna är även ett underlag för att återställa data efter förändringar. Den övervakning och loggning som görs ska följa alla relevanta lagkrav. Alla användare ska känna till förekomsten av loggning.

Den minsta omfattningen systemens loggar ska vara:

- datoridentitet
- datum, tid och detaljer om viktiga händelser
- användaridentitet
- avvisade försök till systemåtkomst
- ändrad systemkonfiguration
- utnyttjande av särskild åtkomsträtt: privilegierade konton som admin, root och supervisor
- larm från styrsystemen för åtkomst
- avstängning av skyddssystem: antivirus, IDS etcetera

Kommentar: Punkterna ovan är en blandning av händelser och beskrivning av vilken information en logg ska innehålla

Detaljerad information samt anvisningar för användning och övervakning av loggfiler framgår av rutiner.

Gallring av E-postloggar

För utförlig information om gallringsfrist, se dokumenthanteringsplan IT-enheten på IN.

Ansvar

Systemägare
För systemens loggar ska systemägare besluta om:

- vad som ska loggas utöver kraven på minsta omfattning enligt ovan
- hur ofta loggarna ska analyseras

- vem som utför och ansvarar för att analysera loggarna
- hur länge loggarna ska sparas
- hur loggarna ska förvaras

IT-enheten
IT-enheten ska tillhandahålla:

- systemstöd för loggning
- kunskap i och omkring loggning
- analystjänster
- övervakning att uppsatta loggningskrav uppfylls

Relaterade rutiner

Rutin för att administrera och hantera loggar.

Rutin för förvaring av loggar.

Rutin för återläsning av loggar.

Rutin för test och kontroll av loggar.

Rutin för att analysera loggar.

Rutin för gallring av e-postloggar

Rutin vid begäran om e-postloggar

2.12 Åtkomst till system och nätverk

Syfte: Att styra användarnas åtkomst till information, system, nätverk och nätverkstjänster samt upplysa användarna om deras ansvar vid datoranvändning. En korrekt hantering av lösenord höjer säkerheten avsevärt.

Behörighet

Nyköpings kommuns IT-miljö är utrustad med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. Användarnas behörigheter tilldelas utifrån arbetsuppgifter och beslutas av närmaste chef samt verkställs av systemansvarig.

Inloggning

Den anställde tilldelas ett initialt lösenord för åtkomst till nätverket och systemet. Lösenordet ska bytas till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst.

Lösenord är strängt personliga och ska hanteras därefter. Användarkontot är personligt och får inte göras tillgängligt för andra. Det får således inte lånas ut och den anställde ansvarar alltid för hur de egna kontona används.

Som användare i ett system lämnar man spår efter sig när inloggning sker och arbete utförs i systemen. De loggningsfunktioner som finns i systemen används för att spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att oskyldiga misstänks i fall oegentligheter inträffar.

Efter tre misslyckade försök att logga in spärras kontot. Om inloggning inte är möjlig ta kontakt med IT-enheten eller systemansvarig för att få ett nytt tillfälligt lösenord.

Om lösenord är bortglömt tillhandahålls ett nytt tillfälligt lösenord av IT-enheten.

Lösenord

För lösenord till nätverk (Active Directory) gäller att det ska:

- initialt vara 8 slumpade tecken långt
- vid byte, bestå av minst 8 tecken
- vara en blandning av stora och små bokstäver, siffror och specialtecken
- inte återanvändas
- bytas var 120:e dag

Produktrelaterade lösenord och standardlösenord med höga behörigheter ska förvaras inlåsta.

Styrning av åtkomst för anställda inom IT-enheten

Användning av verktyg eller hjälpmedel som gör det möjligt att kringgå eller åsidosätta säkerhetssystem och behörighetsskydd ska föregås av godkännande av IT-chefen.

Användarkonto

Användarkontot skapas enligt automatisk rutin för användarkonto.

Gallring av användarkonto

För utförlig information om gallringsfrist, se dokumenthanteringsplan IT-enheten på IN.

Lösenordshantering

Användaren är själv ansvarig för att hålla sina lösenord hemliga och för att välja tillräckligt säkra lösenord.

Ansvar

Systemägaren
Rutiner för administration och uppföljning av behörigheter ska upprättas av systemägaren.

Systemansvarig
Systemansvariga är ansvariga för att regler om administration och uppföljning av behörigheter följs.

Respektive Chef
Beslut om anställds behörighet till IT-system ska tas av divisionschef, chef för central enhet/avdelning eller annan person som är utsedd av divisionschef eller chef för central enhet

Beslut sker efter samråd med systemägaren eller systemansvarige. Redovisning av beslutade behörigheter ska dokumenteras enligt fastställd rutin.

IT-enheten
IT-enheten ansvarar för att det finns en upprättad översikt av säkerhetsarkitekturen för det interna nätverket och kommunikationsanslutningar samt att denna översikt hålls uppdaterad. IT-enheten ansvarar för administrationen av användaridentiteterna för e-post och användarkonto. Samtidigt som en användare tilldelas en användaridentifikation ska användaren också tilldelas en elektronisk e-postlåda och en personlig mapp för dokumentlagring på server.

Relaterade rutiner

Rutiner för användarkonto.

Rutiner för lösenord.

Rutin för autentisering av externa anslutningar.

Rutin för anslutning av utrustning till interna och externa nätverk.

Rutin för anslutning av externa nätverk till Nyköpings kommuns eget nät med ingående säkerhetsfunktioner, autentisering etcetera.

Rutin för anslutning av trådlösa nät.

Rutin och råd kring säkerhet vid Internetanslutning.

Rutin för meddelande om förändringar till Ineras kundservice

Rutin för att rapportera förändringar till Ineras kundservice

2.13 Distansarbete och mobil utrustning

Syfte: Att säkerställa informationssäkerheten vid användandet av mobil utrustning samt övrigt distansarbete.

Hantering av bärbara datorer och dess uppkoppling mot det interna nätverket ska vara reglerat.

För utrustning som används för distansarbete ska det beaktas att den kan utgöra en säkerhetsrisk och att det på dessa inte får lagras sekretessbelagd information. Undantag kan göras om lagringsmedia har godkänd kryptering och godkännande från verksamhetsansvarig chef.

Utrustning som används utanför Nyköpings kommuns lokaler måste skyddas mot brand, stöld och otillbörlig användning. Utrustningen tillhör Nyköpings kommun och ska enbart användas för uppgifter som förknippas med Nyköpings kommuns verksamhet.

Ansvar

Systemägare
Systemägare beslutar om information i ett system ska få hanteras på distans med stationär eller mobil utrustning

Verksamhetsansvarig chef
Verksamhetsansvarig chef beslutar om medarbetaren ges möjlighet till att arbeta på di-stans med stationär eller mobil utrustning.

IT-Enheten
IT-enheten ansvarar för att tillhandahålla tjänster och utrustning för distansarbete.

Anställd
Alla anställda ansvarar för att beakta säkerheten vid arbete utanför Nyköpings kommuns lokaler. Varje anställd ska vid distansarbete:

- iaktta försiktighet när mobil utrustning används
- skydda utrustning och information mot brand, stöld och otillbörlig användning
- enbart använda Nyköpings kommuns utrustning

Relaterade rutiner

Rutin för distansarbete.

Rutin att kryptera filer.

2.14 Anskaffning och underhåll av informationssystem

Syfte: Att vid inköp och utveckling samt vid uppdatering eller förändring av system säkerställa att sekretess, tillgänglighet, riktighet och spårbarhet uppmärksammas.

För varje informationssystem som bedöms vara viktigt för verksamheten ska:

- en systemsäkerhetsanalys upprättas som innehåller systemets samlade krav på informationssäkerhet
- en systemägare och systemansvarig utses
- rutiner för systemets förvaltning och underhållsplan i enlighet med förvaltningsmodellen finnas

Inför nyanskaffning och införande av ett informationssystem ska verksamhetsansvarig chef i samråd med IT-enheten utforma en projektplan för införandet.

Vid överlämnandet från införande, eller utveckling och test till drift och förvaltning, ansvarar den person som är ansvarig för nyanskaffningsprojekt tillsammans med tilltänkt systemägare. Beslut om tidpunkt från vilket systemet övergår från projekt till förvaltning fattas av systemägare. I och med detta övergår ansvaret till systemansvarig som då också övertar all dokumentation och upprättar en systemsäkerhetsanalys.

Förslag om önskemål på förändringar i systemet hanteras i enlighet med rutin för förändring. Arbetet bedrivs enligt Nyköpings kommuns modell för införande och utveckling av systemen.

Relaterade rutiner

Rutin, upphandling av system/program.

Rutin, införande av nytt system/program.

Rutin, patchning och uppdatering.

Rutin, avveckling av uttjänta system.

Rutin, förändring (omfattande).

2.15 Hantering av incidenter

Syfte: Att säkerställa att informationssäkerhetsincidenter och svagheter hos informationssystem rapporteras så att korrigerande åtgärder kan vidtas i rätt tid. Hanteringen av en incident ska ske på ett konsekvent och effektivt angreppssätt.

Om misstanke finns att en användaridentitet använts av obehörig eller att en användare har varit utsatt för någon annan typ av incident ska följande vidtas:

- notera när användaren senast var inne i systemet och när incidenten upptäcktes
- omedelbart anmäla till verksamhetsansvarig chef och IT-enheten
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på informationen har påverkats eller om informationen har kommit i orätta händer
- upptäckta fel och brister i system ska rapporteras till systemansvarig eller till IT-enheten

Nyköpings kommun har programvaror för viruskontroll både i klienterna och i nätverket men kan ändå drabbas av så kallad skadlig kod. Om misstanke finns att datorn innehåller virus ska arbetet avbrytas och IT-enheten omedelbart kontaktas! Anmälan sker per telefon eller besök, inte per e-post.

Mobila enheter som till exempel mobiltelefoner kan lätt bli virusbärare eftersom de används för att överföra data mellan olika datorer. Var noga med att den dator som ansluter en mobil enhet har ett uppdaterat antivirusprogram.

Ansvar

Respektive chef
Respektive chef ansvarar för att informera sin personal om korrekt hantering vid misstanke eller iakttagelse av en incident. Chefen ska även ta emot anmälan om inträffade incidenter från de anställda och vara IT-enheten behjälplig med nödvändig information.

IT-enheten
IT-enheten ansvarar för att registrera alla incidenter och åtgärda dem enligt Tillgänglighetsgarantier för tjänsterna i Nyköpings Kommuns Tjänstekatalog IT.

Anställd
Samtliga anställda har ansvar att rapportera incidenter, fel och brister.

Relaterade rutiner

Rutiner för att analysera loggar.
IT-säkerhetsrutin informationssäkerhetsincidenter, hanteringsplan.
Rutin för att rapportera incident till Ineras kundservice

2.16 Kontinuitetsplanering

Syfte: Att motverka avbrott i organisationens verksamhet samt att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel eller extraordinära händelser. Syftet är även att säkra att återstart kan ske inom en rimlig tid.

Det ska inom Nyköpings kommun finnas rutiner som säkerställer att IT-stödet fungerar kontinuerligt och utan oplanerade avbrott. Om avbrott inträffar ska det finnas planer och rutiner för hur verksamheten ska bedrivas i ett incident- eller extraordinärt läge.

I handlingsplanen för extraordinära händelser ska det för varje system finnas uppgifter om:

- acceptabel avbrottstid som endast orsakar måttlig sänkning av servicenivån
- maximalt tillåten avbrottstid innan ett reservsystem ska tas i drift
- krisorganisation och larmning
- ansvar och befogenheter vid ett extraordinärt läge
- åtgärder vid extraordinärt läge
- prioriteringsplan för reducerad drift och återuppbyggnad
- plan för återuppbyggnad och återgång till normal drift
- regler för vidmakthållande av krisplanen
- plan för utbildning och övning

Se gällande dokumentation ”Handlingsplan för extraordinära händelser”.

Ansvar

Framgår av dokumentet ”Handlingsplan för extraordinära händelser”.

Relaterad rutin

Handlingsplan för extraordinära händelser.

2.17 Kontroll av efterlevnad och revision

Syfte: Att säkerställa att handlande sker i enlighet med riktlinjer, policy, interna rutiner och andra säkerhetskrav.

Revisioner sker löpande inom Nyköpings kommuns alla IT-system.

Områden som är av särskild vikt att beakta efterlevnaden av är:

- Personuppgiftslagen
- Offentlighet- och sekretesslagstiftning
- Upphovsrättslagen
- Bokföringslagen

Information, datorresurser, datornät, kringutrustning och konton ägs och drivs av Nyköpings kommun. Detta innebär att all information som finns i datorerna och systemen är Nyköpings kommuns egendom. Arbetsgivaren har rätt att kontrollera vad som lagras på kommunens datorer samt att återställa infrastruktur och data i enlighet med kommunens rutiner.

Om någon förtroendevald, anställd, personal hos externa utförare eller kontrakterad personal bryter mot vad som anges i policy, riktlinjer och andra styrande regelverk betraktas det som en förseelse och kan bli föremål för disciplinära åtgärder.

Relaterade rutiner

Internrevisionen.

Rutiner för besiktning av användarnas efterlevnad.

3 Riktlinjer för drift och förvaltning

3.1 Drift och förvaltning av kommunens IT-resurs

Systemdokumentation

Systemägande förvaltning ska upprätta en systemdokumentation för ägda system. Systemdokumentationen ska bland annat innehålla:

- översiktlig beskrivning av hur IT-systemet tekniskt är uppbyggt
- vilka delar IT-systemet består av och hur dessa samverkar och kommunicerar
- systemöversikt
- säkerhetsrutiner
- driftdokumentation
- systemhistorik
- automatiskt skapade poster

Dokumentation av förvaltningsorganisation

Förvaltningsorganisationen ska vara dokumenterad för respektive system. Dokumentationen ska skickas till IT-enheten.

Systemägare

Systemägaren är övergripande ansvarig för ett informationssystem och ytterst ansvarig för informationssystemets effektiva användning och utveckling i verksamheten.

Varje systemägare ansvarar för säkerheten i egna system. Säkerhetsnivå och skyddsåtgärder ska fastställas utifrån bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder ska väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet. Rutiner för förvaltning och datasäkerhetsarbete ska dokumenteras och kontinuerligt aktualiseras.

Systemägaren ansvarar för:

- att analys av säkerhetsbehovet genomförs med hänsyn till IT-systemets informationsinnehåll och verksamhetskrav. Säkerhetskraven ska anges med inriktning på tillgänglighet, riktighet, sekretess och spårbarhet
- att riktlinjer för behörighetstilldelning utarbetas
- att nödvändiga tillstånd finns som krävs av datainspektionen

- att en systemansvarig utses
- att vid behov utse systemadministratör
- att information om IT-säkerhet kommuniceras till samtliga användare av IT-systemet

Systemansvarig

För varje system utser systemägaren en systemansvarig. För komplexa system kan systemägaren utse mer än en systemansvarig. Systemägaren utser då en av de systemansvariga att vara övergripande ansvarig för systemet och för koordinationen mellan de systemansvariga. För system som inte har någon systemadministratör utsedd ansvarar systemansvarig även för systemadministratörens arbetsuppgifter.

Systemansvariges uppgift är att vara länk mellan organisationens drift av verksamhetssystem och systemleverantören.

Systemansvarig ansvarar för tilldelning av åtkomsträttigheter till lokala system samt ansvarar för uppföljning av tilldelade behörigheter. Tilldelning och uppföljning ska följa de riktlinjer som systemägaren har fastställt.

Systemansvariges ansvar innebär att:

- ansvara för insamling av ändringsförslag samt ta initiativ till vidareutveckling och underhåll
- initiera uppdateringar
- organisera systemförvaltning
- samordna verksamhetsbehov
- ansvara för utbildningsinsatser i systemet
- inneha systemkunskap
- följa systemets kvalitet genom löpande uppföljning
- samordna olika aktörer: systemadministratör – leverantör – IT-enheten
- ha kunskap om verktyg för systemet
- samordna systemförvaltningen mellan divisioner och de centrala enheterna
- se till att användar- och systemdokumentation finns och är aktuell
- se till att kopplingar till andra system fungerar
- att ansvara för utbildningsinsatser gällande informationssäkerhet

- att följa systemets kvalitet, framför allt utifrån en informationssäkerhetsaspekt, genom löpande uppföljning

Systemadministratör

De system som har delsystem (moduler) bör ha en eller flera systemadministratörer som administrerar den verksamhetsspecifika delen av systemet. Systemägaren utser och anger antal systemadministratörer. Systemadministratörens ansvar innebär att:

- stödja användaren
- administrera verksamhetsanpassning i systemet
- administrera användare i det verksamhetsspecifika delsystemet
- initiera förändringar i det verksamhetsspecifika delsystemet

Teknisk systemansvarig

För den tekniska driftsäkerheten ska en teknisk systemansvarig finnas utsedd. Teknisk systemansvarig utses av IT-chefen och ansvarar för:

- att analyser av den tekniska säkerheten genomförs med hänsyn till tillgänglighet, riktighet, sekretess och spårbarhet, samt att påvisade brister åtgärdas
- att systemägarens säkerhetskrav uppfylls tekniskt
- att säkerhet och behörighet till nätverket och dess servrar uppfylls
- att verkställa uppdateringar av applikationerna i servern efter beställning
- att driftdokumentation finns och uppdateras

Alla användare

Alla anställda ska vara medvetna om informationssäkerhetsfrågornas betydelse så att de kan ta ansvar för att den personliga IT-användningen kan ske med god säkerhet.

Alla användare ska ha tillgång till informationsmaterial så att de kan ta eget ansvar för informationssäkerheten vid den personliga IT-användningen.

Relaterad rutin

Dokumentmall för förvaltning av drift av system.

3.2 Utrustning

Syfte: Att förändra synen på IT-utrustning så att den betraktas som kommunens arbetsverktyg. Det ger möjlighet att styra användningen, livscykeln och att en striktare standardisering av utrustningen uppnås.

IT-enheten äger IT-utrustningen (dator, skärm och skrivare).

Varje dator samt skrivare ska vara förtecknad och märkt ”Nyköpings kommun”, samt ha ett unikt inventarienummer. Dessutom ska varje IT-utrustning vara stöldskyddsmärkt. Det ska framgå av en förteckning vilken verksamhet som ansvarar för IT-utrusningen och vem som använder den. Omflyttning och överlåtelse av utrustning får inte ske utan att IT-enheten meddelas.

För utrustning du förfogar över, det vill säga stationär, dockningsbar PC eller bärbar PC med tillhörande utrustning gäller:

- fysiska ingrepp får endast utföras av IT-enheten
- fel ska omgående anmälas till IT-enheten
- all installation och konfiguration får endast utföras av IT-enheten
- arbete mot Nyköpings kommuns IT-miljö får endast utföras på ett av IT-Enheten anvisat sätt

Mobiltelefoner registreras med ett unikt nummer som möjliggör att telefonen spärras vid eventuell förlust av telefonen.

Endast IT-utrustning (datorer, skrivare, scanner, kameror och dylikt) och data och teleförbindelser som är verifierad av IT-enheten, får användas inom Nyköpings kommun eller anslutas till Nyköpings kommuns IT-miljö.

Ansvar

Verksamhetschef
Respektive verksamhetschef ansvarar för att, inom sin verksamhet, ha kontroll över den utrustning som är registrerad på verksamheten.

IT-enheten
IT-enheten ansvarar för att, i enlighet med gällande riktlinjer, upprätta förteckning över IT-utrustning (datorer, skärmar, skrivare) och mobiltelefoner som köps in till Nyköpings kommun. Denna förteckning ska hållas uppdaterad.

IT-enheten ansvarar för att hantera utrustning och applikationer när fel uppkommer samt att ta emot media och IT-utrustning (datorer, skärmar och skrivare) för korrekt avveckling. Denna avveckling ska genomföras enligt rutinerna.

Respektive chef
Alla chefer ansvarar för att informera den egna personalen om riktlinjerna samt att de ges möjlighet till utbildning.

Anställd
Alla anställda ska hantera utrustningen i enlighet med dessa riktlinjer.

Relaterad rutin

Rutin för beställning av IT-utrustning.

Rutin för avvecklingen av utrustning.

Rutin för utrustning som flyttas.

Rutin för arbetsplatsen.

Rutin för utrustningens konfiguration.

3.3 Privat användning av kommunens IT-resurs

Syfte: Att klargöra privat användning av kommunens IT-resurs.

Anställda får använda kommunens IT-resurs för att skicka och ta emot enstaka privata e-brev, besöka sociala medier samt för tillfällig användning av Internet för att exempelvis utföra enklare bankärenden.

Denna användning får inte vara relaterad till någon form av näringsverksamhet eller omfattande hobbyverksamhet.

Användaren ska uppmärksamma risken med virus vid kommunikation via Internet, särskilt gäller detta virus i e-postbilagor. Att använda ett privat e-postkonto i tjänsten och via webbläsare hämta in e-post med bilagor till arbetsdatorn utgör ett direkt säkerhetshot mot kommunens IT-resurs.

All användning som bryter mot legala regelverk eller ligger utanför normalt gott uppträdande inom en offentlig verksamhet är ej tillåten.

Den anställde ska inte lagra privat material i kommunens IT-resurs.

Relaterad rutin

Rutiner för användning av sociala medier.

3.4 Stöldskydd och försäkring

Syfte: Att försäkra att kommunens utrustning förvaras på ett säkert sätt och att den är försäkrad.

IT-utrustning har högt värde och är därför intressant som stöldobjekt. Ofta kan enkla åtgärder minska risken för stöld. Innehåller utrustningen sekretesskyddad information kan ingen försäkring reparera den skada som uppstår om informationen kommer i orätta händer. Vid hantering av sekretesskyddad information vilar ett stort ansvar på den enskilde användaren.

Stöldskydd av utrustning

All utrustning som inte är av ringa värde ska stöldmärkas och redovisas i en inventarieförteckning. I förteckningen ska det även finnas serienummer och annan information för att identifiera utrustning. IT-enheten håller denna förteckning.

Speciellt viktigt är att portabel datautrustning som bärbara datorer och videoprojektorer hanteras på ett säkert sätt.

Bärbara datorer som innehåller sekretesskyddad information och är placerade i lokaler där stöld är möjlig ska förvaras inlåsta i säkerhetsskåp när lokalen är obemannad. Se även dokumentet Fastighetssäkerhet 8.10.

Försäkring av utrustning

Utrustningen omfattas av villkoren i kommunens försäkringsskydd.

Ansvar

Det är ansvarige verksamhetschef som ansvarar för att utrustningen förvaras på ett säkert sätt och att den har stöldskydd.

Relaterade rutiner

Rutin för stöldskydd av utrustning.

Rutin vid stöld av utrustning.

3.5 Stöld av IT-utrustning

Syfte: Att säkerställa att IT-utrustning anmäls och avregistreras på ett korrekt sätt.

Respektive verksamhet ansvarar för utrustningen och alla kostnader som uppstår i samband med stöld.

Verksamheten är ansvarig för att stöld av IT-utrustning blir anmäld enligt gällande rutiner.

Relaterade rutiner

Rutiner vid stöld av IT-utrustning.

Rutiner för försäkring.

3.6 Lagring av data

Syfte: Att säkerställa att lagringen av data sker på ett effektivt och säkert sätt.

Alla servrar för verksamheterna ägs och förvaltas av IT-enheten, med centrala medel och resurser.

Ett rullande schema ska finnas för kopiering till externt media där månadskopior lagras på annan plats än i en datahall. Data lagrat på lokal disk (C:) ansvarar användaren själv för.

Gallring av hemkatalogen W

Gallring sker i samband med att användarkonto avslutas, dock senast 45 dagar efter att användaren avslutar anställning i kommunen. Gallringen sker enligt manuell rutin.

Relaterade rutiner

Rutin för lagring av data.

Rutin för gallring av användarens dokument i hemkatalogen W

3.7 Säkerhetskopiering

Syfte: Att säkerställa att säkerhetskopiering av data sker på ett säkert sätt.

Filer som lagras på en PC (klienten) försvinner om hårddisken havererar. För att minimera problemen som uppstår vid hårdvaruhaverier ska alla användare som har god kommunikation med servern lagra informationen på denna. Det finns speciella katalogstrukturer på servern där användare har en hemkatalog.

IT-enheten ansvarar för säkerhetskopiering av servrar. När informationsmängden som ska sparas ökar kan informationsklassificeringen användas för att, tillsammans med systemägare, värdera behovet av dagliga säkerhetskopior.

För datorer som inte är anslutna till nätverk med server, eller anslutna över förbindelser som ej klarar säkerhetskopiering, ansvarar användaren för säkerhetskopiering. IT-enheten bistår med anvisningar och tekniska lösningar.

3.8 Programvaror/applikationer

Syfte: Att säkerställa att Nyköpings kommun inte har olicensierad programvara i sin IT-miljö samt att applikationen är verifierad så att den inte påverkar kommunens IT-miljö på ett negativt sätt

Programvaror (applikationer)

Programvaror ska verifieras och godkännas samt installeras av IT-enheten eller av IT-enheten godkänd person. Egna program får inte installeras i kommunens datorer. Det är inte tillåtet att kopiera eller använda Nyköpings kommuns program utanför kommunens verksamhet. Om behov finns av ytterligare programvaror eller hårdvara ska det anmälas till närmaste chef. Inga nöjesprogram, som till exempel spelprogram eller externa skärmsläckare, får installeras i kommunens datorer.

Originalmedia

Programvara på originalmedia ska efter installation (eller kopiering) förvaras av respektive verksamhet i ett brandsäkert kassaskåp. Parameterinställningar för programvaror i servrar, routrar och arbetsplatsdatorer ska kopieras och förvaras av IT-enheten på liknande sätt.

Demoprogram och media

Stor restriktivitet gäller för installation av demoprogram. Består demon av ett program ska användaren först kontakta IT-enheten för diskussion om lämpligheten av installationen. Endast demoprogram direkt relaterade till användarens arbetsuppgifter får installeras.

Extern lagringsmedia

Innan media från extern källa sätts in i datorn ska användaren försäkra sig om att datorns antivirusprogram är aktivt i realmode och att senaste virussignaturfil är nerladdad i datorn. I detta sammanhang anses den anställdes hemdator som extern källa.

Hantering av programlicenser

Programlicenser ska förvaras så att de inte är tillgängliga för utomstående. Licensavtal ska förvaras samlat så att de är återsökningsbara. En förteckning över verksamhetens licenser ska finnas med uppgifter om antalet licenser och hur många licenser som används.

Relaterade rutiner

Originallicenser (licensdokument) ska förvaras hos IT-enheten i ett brandsäkert kassaskåp.
Register över antal licenser och antal licenser som används ska finnas.

3.9 Tillträde och behörighet till kommunens IT-resurser

Syfte: Att tydliggöra hur medarbetare får tillträde och behörigheter till Nyköpings kommuns IT-resurser.

Respektive chef för division, centralenhet eller avdelning har ansvaret för att ansvarsförbindelse för användning av dator-, nät- och systemresurser i Nyköpings kommun finns.

Behörighet

Beslut om anställds behörighet till IT-system ska fattas av divisionschef, chef för central enhet eller avdelning, eller annan person som är utsedd. Beslut sker efter samråd med systemägaren. Redovisning av beslutade behörigheter ska ske skriftligt på ett för systemet speciellt formulär och vara attesterade av divisionschef, chef för central enhet eller avdelning eller den som är utsedd.

Rutiner för administration och uppföljning av behörigheter ska upprättas av systemägaren. Systemansvariga är ansvariga för att regler följs.

Det ska speciellt observeras att behörigheter omgående ska förändras när förutsättningarna förändras, exempelvis när en användare slutar sin anställning, får nya uppgifter eller när nya användarresurser eller väsentliga funktioner läggs till i systemet.

Användaridentiteter

Varje användare av något av kommunens IT-system ska ha en personlig användaridentitet. Nyuppläggning, uppdatering och borttagande av användaridentifikation beslutas av den verksamhet där personen är anställd. IT-enheten ansvarar för administrationen av användaridentiteterna för e-post och användarkonto.

Vid tilldelning av användaridentifikation erhålls en e-postlåda och en personlig mapp för dokumentlagring på server. Däremot läggs inga behörigheter till verksamhetssystemen upp av IT-enheten.

Användarrättigheter för verksamhetssystem rekvireras från systemägande förvaltning enligt den ordning som bestämts i dokumentationen för systemet. All utdelning av rättigheter ska dokumenteras.

3.10 E-post

Syfte: Att säkerställa att e-post hanteras så att Nyköpings kommun inte bryter mot offentlighetsprincipen eller andra lagar och regler. Samt säkerställa att sekretessbelagd information inte distribueras via e-post.

Användaren ansvarar själv för innehållet i sin e-postbrevlåda som han eller hon ansvarar för och för att bevaka inkommande post. Notera att elektronisk post är att jämställa med vykort. Tänk på att datorpost aldrig helt kan skyddas mot obehörig åtkomst

För att inte känslig information, exempelvis sekretessbelagd, ska komma i fel händer, får inte sådan information skickas via e-post.

Arkiv- och offentlighetslagstiftningen gäller elektronisk post och inlägg i sociala medier och användningen får inte strida mot dessa. Användaren är därför skyldig att vidarebefordra till registrator, datorpost som han eller hon mottagit i tjänsten och som inte uppenbart är av ringa betydelse för kommunens verksamhet.

Vad gäller e-post är det viktigt att varje användare hanterar detta verktyg på ett korrekt sätt. Det ska hanteras på ett sådant sätt att inte spridning av datavirus riskeras.

Man ska undvika att använda e-posten för interna gruppsändningar och vara restriktiv med att skicka kännedomskopior som belastar systemet i onödan.

För att minska mängden skräppost har ett så kallat spamfilter installerats. E-post från kända spamavsändare sorteras bort. Vissa e-postbrev märks som misstänkta, dessa brev får användaren själv avgöra om de ska tas bort.

Din e-post är också möjligt att hämta via Internet, http://epost.nykoping.se

E-postkonto

Användaren har ett maximalt utrymme för den totala postlådan. En varning läggs ut innan postlådan är fylld. Om inte rensning sker av gammal post går det inte att ta emot eller sända nya brev. Den e-post som berörs kan ligga i inkorgen, borttaget, skickat eller någon annan mapp i din postlåda.

Gallring av E-postkonto

För utförlig information om gallringsfrist, se dokumenthanteringsplan IT-enheten på IN.

Relaterade rutiner

Rutiner för e-postkonto.
Rutiner för byte av e-postadress.
Rutiner för användning av sociala medier.

3.11 Sociala medier

Syfte: Att säkerställa att sociala medier hanteras så att Nyköpings kommun inte bryter mot offentlighetsprincipen eller andra lagar och regler. Samt säkerställa att sekretessbelagd information inte distribueras via sociala medier.

Användaren ansvarar själv för innehållet på den plats i sociala medier som han eller hon är ansvarig administratör för.

Arkiv- och offentlighetslagstiftningen gäller inlägg i sociala medier och användningen får inte strida mot dessa. Användaren är därför skyldig att vidarebefordra till registrator, inlägg i sociala medier som han eller hon mottagit i tjänsten och som inte uppenbart är av ringa betydelse för kommunens verksamhet.

Relaterad rutin

Rutiner för användning av sociala medier.

3.12 Drift av nät och servrar (system)

Syfte: Att säkerställa att drift och underhåll leder till att minimera avbrott samt att säkerställa att servrar är placerade så att dessa erhåller ett korrekt skydd.

Nät- och serverutrustning som ansluts till Nyköpings kommuns nät kan utgöra en säkerhetsrisk om drift och underhåll åsidosätts.

Särskilda föreskrifter finns för:

- säkerhet för enskilda datorsystem
- kryptering av datatrafik (SSL, VPN)
- e-postservrar
- identifiering av användare

Kommungemensamma underliggande system

IT-enheten ansvarar för drift och teknisk systemförvaltning av kommunövergripande underliggande system och nätverk. Telefonsupport och felanmälan tillhandahålls under kontorstid av tilldelad systemansvarig, som i sin tur kontaktar IT-enheten vid behov.

För information om prioritetsklasserna, som nämns under felavhjälpning, hänvisas till dokument ”Tillgänglighetsgarantier”. Den finns att hämta på IT-enhetens informationssida på IN.

Placering av servrar

Samtliga servrar ska vara placerade i IT-enhetens datorhall.

Datahall

Servrar och kommunikationsutrustning förvaras i utrymme som klarar krav på yttre säkerhet, (brand, larm och obehörigt tillträde) samt miljö (klimat och ventilation). Tillträde till datahall ska hållas begränsat och avgörs av IT-Enheten. Som regel har endast personal från IT-Enheten, Kommunfastigheter och vaktbolag tillträde. Övriga externa personer som till exempel elektriker och konsulter ges tillträde av IT-enheten.

Internt nätverk

Kommunens ”inre” nätverk består av olika fysiska nät; fiber, koppar eller radio. Nätverken är skilda åt med så kallade routers. Dessa konfigureras så att behörighet kan tilldelas på nätnivå, exempelvis för att skilja utbildningsnät från administrativt nät. Detta beslutas och utförs av IT-Enheten.

Ansvar

För respektive system finns teknisk systemansvarig, som ansvarar för drift av system.

Relaterade rutiner

Rutiner för daglig övervakning.

Rutiner för loggning av vitala aktiviteter i systemen.

Rutiner för incidentrapportering.

Rutiner för information vid inträffad incident.

Rutiner för incidenter som uppstått genom händelser som är eller kan vara brott mot svensk lag.

Rutiner för driftsinformation om driftstörningar, planerade avbrott, servicefönster, med mera.

3.13 Upphandling

Syfte: Att upphandling av IT-system, IT-utrustning och IT-tjänster uppfyller Nyköpings kommuns policy och riktlinjer när det gäller verifiering av produkter och tjänster samt informationssäkerhet. Samt att begränsa antal system.

Vid upphandling och utveckling av IT-system och IT-tjänster ska säkerhetsaspekter beaktas.

IT-enhetens roll vid anskaffning av system är att verifiera funktionalitet i förhållande till kommunens IT-miljö och säkerhetsaspekter.

IT-enheten bevakar även systemets behovsbeskrivning mot andra system som har samma funktionalitet.

IT-enheten kan om verksamheten så önskar hjälpa till med krav- och behovsanalys enligt IT-enhetens informationssidor på IN.

Leverantörers och konsulters tillgänglighet till sekretessbelagd information ska uppmärksammas och regleras vid upphandling av nya system och vid upphandling av uppgraderingar.

Relaterad rutin

Rutin för upphandling.

3.14 Utbildning och information

Syfte: Att höja kompetensen hos anställda och förtroendevalda för att öka effektiviteten i nyttjandet av kommunens IT-resurser.

IT-resurser blir ett allt viktigare verktyg inom Nyköpings kommuns verksamhet. Det är nödvändigt att anställda, förtroendevalda och studenter har tillgång till utbildning och information för att få en effektiv och säker IT-användning.

IT-enheten tillhandahåller utbildning för de vanligaste verktygen. Kommunens ledare ska motivera anställda att ta del av dessa.

Systemägare kan föreskriva att användare måste ha genomgått viss utbildning.

Relaterad rutin

Rutin för utbildning och information.

4 Riktlinjens genomförande

4.1 Omfattning och volymer

Dessa riktlinjer gäller samtliga anställda, förtroendevalda, inhyrd eller kontrakterad personal inom Nyköpings kommun. Riktlinjerna, tillsammans med policyn för IT-säkerhet, är det styrande regelverket inom Nyköpings kommun. Samtliga dokument finns hos IT-enheten.

4.2 Organisation

Nyköpings kommuns IT-enhet har i uppdrag att utgöra kompetenscentrum i IT-frågor vilket också inkluderar informationssäkerhetsfrågor. Verksamheten inom IT-enheten ska drivas med informationssäkerheten i fokus och med aktivt deltagande i förebyggande informationssäkerhetsarbete. Verksamheter kan få råd och stöd av IT-enheten i det egna informationssäkerhetsarbetet.

IT-enhetens organisation och tjänster finns beskrivna på IN.

Samverkan

Som stöd för informationssäkerhetsarbetet samt drift och förvaltning finns referensforum. I forumen sker informationsutbyte om informationssäkerhetsarbetet samt drift och förvaltning av IT-resurser inom Nyköpings kommun.

Samverkan mellan IT-enheten, divisioner, centrala enheter och avdelningar sker i forum för IT Strategiforum, IT Verksamhetsforum och IT Referensforum.

Ansvar

Divisionschefer, chefer för centrala enheter och avdelningar samt enhetschefer ansvarar för att personalen inom verksamheterna får nödvändiga kunskaper för att IT-resurser ska kunna utnyttjas på ett säkert och effektivt sätt.

Divisionschefen respektive chefen för central enhet är ansvarig för informationssäkerheten. Vid varje division och central enhet ska det finnas en kontaktperson i informationssäkerhetsfrågor som kan medverka i information och erfarenhetsutbyte i dessa frågor.

5 Uppföljning och revidering av riktlinjen

5.1 Brott mot regelverket

Om någon anställd eller kontrakterad personal bryter mot policyn, riktlinjer och andra styrande regelverk betraktas det som en förseelse. Detta kan leda till disciplinära åtgärder eller uppsägning vid grov försummelse.

Kommundirektören ansvarar för rapportering om brott mot regelverket när det gäller förtroendevalda.