



VÄGLEDANDE RÅD OCH BESTÄMMELSER FÖR SÄKERHET IT-SÄKERHETSINSTRUKTION FÖRVALTNING

Fastställd av kommunstyrelsen 2013-05-07, § 98

Organisation och ansvar

Förvaltningschef eller avdelningschef är systemägare och ansvarig för IT-system som stödjer den egna verksamheten. Systemägare för Teknisk infrastruktur IT är IT-chef.

Ansvarsfördelningen ska medverka till att stödja verksamheten och uppfylla informationssäkerhetspolicyns mål. Detta innebär att ett IT-system, med alla dess delar, är en resurs i en verksamhet på samma sätt som personal och lokaler.

Det övergripande ansvaret för kommunens IT-system åvilar kommunstyrelsen.

IT-Rådet

IT-rådet består av förvaltningschefer och centrala IT med mandat för beslut. Dess uppgifter är:

- beslut av verksamheternas behov av IT-stöd efter underlag från systemförvaltarna
- beslut av mål för IT-säkerhetsarbetet och kommunens säkerhetsinstruktioner efter underlag från IT-säkerhetssamordnaren
- utformning av kommunens långsiktiga IT-planering
- samordning av systemägarnas krav på Teknisk infrastruktur
- beslut av sekretessförbindelser för konsulter och serviceföretag efter underlag från centrala IT och IT-säkerhetssamordnaren
- beslut av kommunens kontinuitetsplan
- ledningsgrupp vid större IT-säkerhetsincident
- säkerställa att systemen fungerar tillsammans med samverkande IT-system

Systemägare

Systemägaren har ansvar för bland annat:

- att inför verksamhetsplaneringen initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-rådet
- att externa leverantörer av tjänster och produkter blir informerade om kommunens informations- och säkerhetskrav.
- att i en systemsäkerhetsanalys fastställa eventuella tilläggskrav utöver basnivån.
- att organisation och befattningar som rör systemet möter aktuella behov
- att fastställa IT-systemets dokumentation och användarhandledning
- att fatta beslut om utveckling av IT-systemet vad gäller nya funktioner och samverka med IT-chef då systemförändringar aktualiseras
- att erforderliga licenser och avtal finns



- att i samverkan med IT-chef fastställa kontinuitetsplan för verksamhetssystemen
- att driftgodkänna verksamhetssystemet

Systemförvaltare

Systemförvaltare utses av systemägaren och är den person som har ansvaret för den dagliga användningen av IT-systemet. Systemförvaltaren ansvarar för systemförvaltning utifrån systemägarens direktiv vad gäller tillämpning i verksamheten, användarnas krav och behov samt att förväntade nyttoeffekter realiserar. Systemförvaltaren skall ha en djup kunskap om den verksamhet som systemet ska stödja samt övergripande kunskap om tekniken som tillämpas i systemet. Vidare skall systemförvaltaren säkra att det finns en fungerande förvaltnings- och utvecklingsmodell, där alla ingående parter samverkar kring systemets användning och utveckling. Parterna är primärt systemägare, administratörer, användargrupper, applikationsleverantör och driftleverantör.

Organisation

Systemförvaltaren rapporterar till systemägaren eller till en styrgrupp ansvarig för flera system. Systemförvaltaren driver sina egna forum för att säkerställa att systemet används och utvecklas på det sätt som bäst gynnar verksamheten. Systemförvaltaren tillhör både kommunens systemförvaltargrupp och förvaltningens systemförvaltargrupp.

Arbetsuppgifter

- säkerställa att det finns ett systemägardirektiv
- säkerställa att det finns en förvaltningsplan inkl. budget för ingående verksamhetsår
- säkerställa att det finns en 2-årig utvecklingsplan inkl. budget
- hålla regelbundna möten med systemets administratörer och användare för att få kunskap om hur systemet fungerar i verksamheten.
- se till att systemdokumentation och media finns tillgängliga och är uppdaterade
- se till att användarhandböcker finns tillgängliga och är uppdaterade
- säkerställa utbildning och att systemet används på rätt sätt i verksamheten
- hantera eventuella behörigheter till systemet (framförallt hantera behörigheter för systemadministratörer)
- se till att avtal finns med applikationsleverantör avseende support och nya releaser
- se till att avtal finns med driftleverantör avseende drift av applikationen
- säkerställa att avtalen mellan applikationsleverantör och driftleverantör hänger ihop
- genomföra kontinuerliga avstämningar med applikations- och driftsleverantör där planer och behov diskuteras.
- fånga upp problem, rapportera och driva dessa gentemot applikationsleverantör och driftleverantör
- koordinera och testa nya releaser av systemet
- se till att systemsäkerhetsanalys genomförs och följs upp.



IT-chef

IT-chef är systemägare för den tekniska infrastrukturen och har det övergripande ansvaret för att de kommungemensamma systemen tekniskt fungerar. IT-chefen ansvarar också för IT-rådets funktion upprätthålls och att samtliga mål och planer tas fram.

IT-säkerhetssamordnare

IT-säkerhetssamordnaren stödjer arbetet med att uppnå informationssäkerhetspolicyns mål. Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering samt deltagande i diskussioner kring metoder, plattformar och IT-system. IT-säkerhetssamordnaren är ett stöd för verksamheterna och är i IT-säkerhetsfrågor direkt underställd säkerhetschefen.

IT-säkerhetssamordnaren ska stödja systemägarna i arbetet med att ta fram Risk och sårbarhetsanalyser. Samordnaren ska även se till att informationsklassningen, lagar ska vara väl kända inom kommunen. Även den interna kontrollen av att verksamheterna följer lagar och bestämmelser ansvarar IT-säkerhetssamordnaren för. Denne ska informera IT-chefen löpande.

IT-incidenthantering

IT-säkerhetssamordnaren ska sammanställa och rapportera till ledningen:

- intrång och försök till intrång
- brott mot lagstiftning och interna regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar.

Behörighetsadministration

Det är nödvändigt att administration av och regler för behörighetstilldelning är klart fastlagda och kända. Detta innebär att:

- endast behörig användare ges åtkomst till ett IT-system
- användares behörighet ska styras utifrån dennas arbetsuppgifter och efter beslut av arbetsledningen
- varje användare ska ha en personlig identitet bestående av login-id och lösenord
- den som är tjänstledig eller av annan orsak har längre frånvaro skall ha sin identitet spärrad
- uppföljning och revidering av tilldelade behörigheter ska ske regelbundet.

Loggning och spårbarhet

Målet är att det i samtliga IT-system ska finnas en säkerhetslogg, som minst registrerar användaridentitet, uppgift om inloggning och utloggning samt datum och klockslag för detta. Systemägarnas övriga krav på säkerhets- och transaktionsloggar ska framgå av de systemsäkerhetsplaner som respektive systemägare upprättar.

Distansarbete

Systemägaren och verksamhetsansvarig chef ska besluta om ett IT-systems information ska få hanteras på distans med stationär eller mobil utrustning.



Tillträdesskydd

IT-chef ska besluta om vilka som ska ha tillträde till kommunens datahall.

Säkerhetskopiering och lagring

Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av de systemsäkerhetsanalyser som respektive systemägare upprättar. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsanalyser för teknisk infrastruktur.

Följande är kommunens basrutiner gällande backup:

- Backup tas varje natt mellan 22:00 -06:00
Backup består av INC backup med TSM på samtliga noder vad gäller OS och applikationer.
Databaser typ EXCH och SQL backas med ON-line agent direkt till TSM Diskpool.
Loggbackup av SQL görs varannan timme.
- Media består av Sekventsiella filer på Diskpool tillhörande TSM Backupserver.
Dessa filer ligger på disk så länge datat är aktuellt. Dessutom finns det en kopia på en sekundär server i annan byggnad.
- TSM arbetar med versions hantering av filer, samt varaktighet efter borttagning från backad nod (Maskin)
Antal versioner: 7 st
Antal dagar som sparas efter borttagning: 60 dagar
- Datat ligger accessbart på TSM Diskpool hela tiden, så länge det inte har tagits bort p.g.a ovanstående regler.
- Backup och restore av förlorat data, som ligger inom ovanstående regler hanteras av EVERY one Outsourcing Services Malmö

IT-säkerhetsutbildning

Systemägare ansvarar för

- att de egna medarbetarna erhåller information och utbildning om innehållet i de systemsäkerhetsplaner de är berörda av
- att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om säkerhetsreglerna för de IT-system de behöver för de egna arbetsuppgifterna.

Varje enskild medarbetare har ett ansvar att påtala det egna behovet av utbildning.