SÄKERHETSFÖRESKRIFTER

FÖR FÖRVALTNING AV IT-SYSTEM

Dokumenttyp Riktlinjer	Förvaltning KSF, stab
Ämnesområde IT	
Ägare/ansvarig IT-strateg	
Antagen av KS 2012-02-08 § 47	Dnr KS/2010:1056
Revisions datum	Giltig fr.o.m.
	Giltig t.o.m.

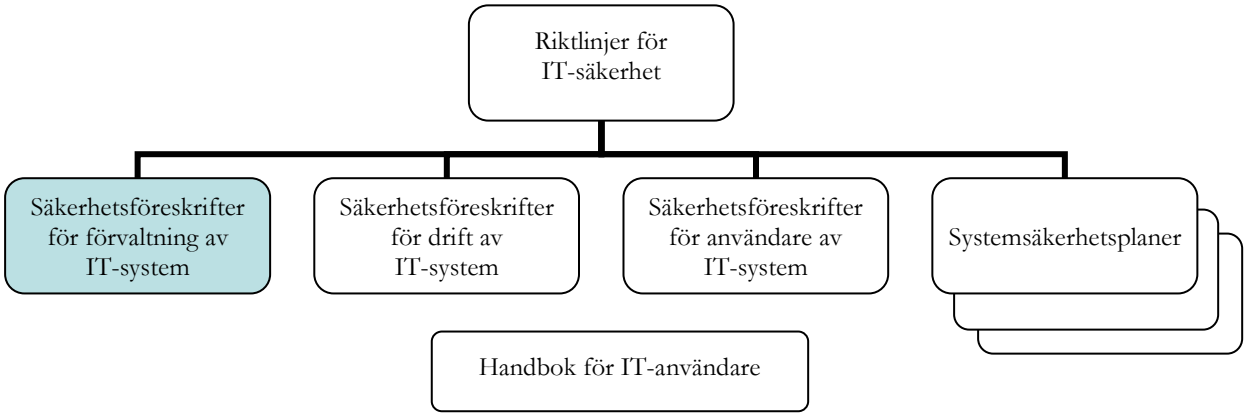
INNEHÅLLSFÖRTECKNING

1 INLEDNING

1.1 Dokumentets roll i IT-säkerhetsarbetet

IT-säkerhet är en del av kommunens lednings- och kvalitetsprocess vilken ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Myndigheten för samhällsskydd och beredskap (MSB) rekommenderade basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet inom Orust kommun.

Styrande dokument för IT-säkerhetsarbetet



Riktlinjerna för IT-säkerhet redovisar kommunstyrelsens beslutade viljeinriktning och mål för IT-säkerhetsarbetet. Detta dokument ”Säkerhetsföreskrifter för förvaltning av IT-system”, utgår från riktlinjerna för IT-säkerhet och syftar till att

- redovisa den interna organisationen för IT-säkerhetsarbetet
- beskriva omfattningen av det ansvar för IT-säkerhetsarbetet som vilar på de roller som ingår i organisationen
- beskriva hur IT-säkerhetsarbetet ska bedrivas
- ange de särskilda rutiner som gäller i tillämpliga fall

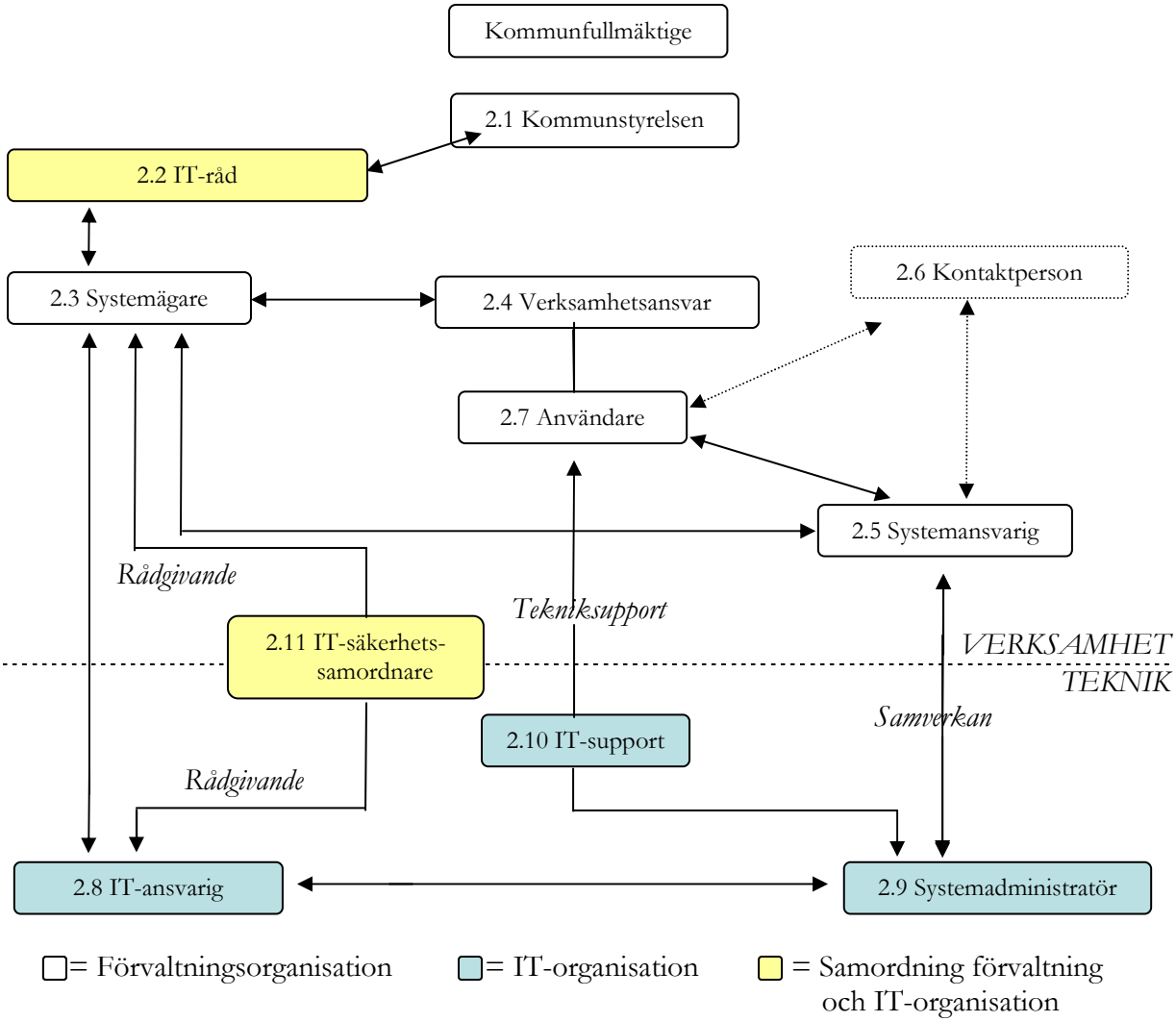
2 ORGANISATION OCH ANSVAR

Ansvaret för informationssäkerheten ska följa linjeorganisationen för varje enskilt IT-system. Utsedd systemägare är ansvarig för de IT-system som stödjer den egna verksamheten.

För den tekniska infrastrukturen är IT-ansvarig systemägare.

Ett IT-system, med alla dess delar, är en resurs i verksamheten på samma sätt som personal, lokaler, kontorsmaterial m.m. Ansvarsfördelning och roller ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla målen i riktlinjer för IT-säkerhet.

Roller inom IT-säkerhetsområdet



2.1 Övergripande ansvar

Det övergripande ansvaret för kommunens IT-system vilar på kommunstyrelsen. IT-rådet identifierar vilka IT-system som är samhällsviktiga och/eller verksamhetskritiska. Systemägare för dessa system ansvarar för att en *systemsäkerhetsplan,* baserad på en risk- och sårbarhetsanalys, upprättas.

2.2 IT-råd

För att uppnå samsyn i IT-frågor finns ett samordnande IT-råd. Gruppen ska hantera och utreda IT-frågor och förbereda dessa för beslut. Kommunchefen leder IT-rådet. Gruppen består utöver den centrala ledningsgruppen av IT-ansvarig, IT-säkerhetssamordnare och informatör.

Inför den årliga verksamhetsplaneringen ska IT-rådet samordna verksamheternas inventerade behov av IT-stöd kommande verksamhetsår (kortsiktigt mål) inom områdena:

- införande (med införande avses alla frågor om nyanskaffning av IT-system)
- systemförvaltning (med systemförvaltning avses samtliga aktiviteter som görs för att verkställa alla typer av förändringar av redan existerande IT-system)
- driftfrågor

- systemavveckling (med systemavveckling avses samtliga aktiviteter som görs för att ett system tas ur drift).

IT-rådet sammanställer behoven i form av förslag till mål för kommande verksamhetsår. Dessa överlämnas för beslut i kommunstyrelsen.

IT-rådets uppgifter i övrigt är att
- utforma förslag till långsiktiga mål för IT-verksamheten
- under pågående verksamhetsår behandla frågor och uppdrag som uppstår inom ovanstående områden (t ex akuta behov, inkomna förslag)
- utforma kommunens IT-kontinuitetsplan
- planera för hur IT-säkerhetsfrågor utifrån genomförda risk- och sårbarhetsanalyser ska hanteras
- ansvara för metod och system för upprättande och underhåll av systemsäkerhetsplaner
- samordna systemägarnas krav på den tekniska infrastrukturen utifrån upprättade systemsäkerhetsplaner
- ansvara för utformning av sekretessförbindelser inklusive konsulter och serviceföretag
- samordna att avtal med annan part som utför tjänst eller uppdrag åt organisationen innehåller en informationssäkerhet som motsvarar organisationens krav
- samordna kompetensutveckling hos verksamhetsansvariga inom områdena IT, juridik och kvalitet
- ansvara för underhåll och revidering av kommunens riktlinjer för IT-säkerhet, säkerhetsföreskrifter för förvaltning av IT-system och säkerhetsföreskrifter för användare av IT-system
- ansvara för upprättande och underhåll av organisationens systemförteckning
- identifiera vilka IT-system som är samhällsviktiga och/eller verksamhetskritiska

2.3 Systemägare

För övergripande system är kommunchefen, eller av denne utsedd person, systemägare. För verksamhetsspecifika system är verksamhetsansvarig, eller av denne utsedd person, systemägare. Systemförteckningen ska för varje given tidpunkt ange utsedd systemägare.

Systemägaren ansvarar för att egna IT-system förvaltas på ett för verksamheten bästa sätt. Vid nyutveckling eller större förändringar av IT-system ska systemägaren alltid på ett tidigt stadium samråda med IT-ansvarig och därefter i IT-rådet. Systemägaren beslutar om IT-systemets införande, förvaltning, drift och avveckling.

Inom ramen för tilldelade resurser ansvarar systemägaren för följande:
- inför den årliga verksamhetsplaneringen, initiera och presentera den egna verksamhetens behov av IT-stöd till IT-rådet
- fortlöpande följa upp att egna IT-system stödjer verksamheten
- delta i och stödja IT-säkerhetsarbetet
- upprätta en systemsäkerhetsplan enligt fastställd mall
- fastställa eventuella tilläggskrav utöver basnivån för IT-systemet i systemsäkerhetsplanen utgående från
  - den information IT-systemet hanterar
  - lagar, förordningar och allmänna råd

  - verksamhetens krav på säkerhet avseende sekretess, riktighet och tillgänglighet
  - hotbilden mot informationen
  - vilka olika behörighetsprofiler som ska gälla
  - omfattning av loggning (trans- och säkerhetsloggar)
  - hur loggar ska följas upp, arkiveras, förvaras och sparas
  - längsta acceptabla tid för driftavbrott och/eller informationsbortfall
  - längsta acceptabla tid för hur snabbt säkerhetskopierat material ska kunna återskapas
- organisation för aktuellt IT-system
- fastställande av IT-systemets dokumentation och användarhandledning
- utbildning som behövs för att hantera IT-systemet
- i samråd med IT-ansvarig, säkerställa att systemet fungerar ihop med samverkande IT-system
- fatta beslut om förvaltning av IT-systemet
- samverka med IT-rådet då större systemförändringar aktualiseras
- föreslå IT-rådet att system som inte är till nytta för verksamheten avvecklas
- behövliga licenser och tillstånd finns
- fastställande av en avbrottsplan för IT-systemet i samverkan med IT-ansvarig
- driftgodkänna IT-systemet

2.4 Verksamhetsansvar

Den som har personalansvar i den dagliga verksamheten ansvarar för den dagliga användningen av IT-systemen för att säkerställa en säker och rationell användning. Ansvaret omfattar även informationen i IT-systemen samt att denna hanteras på ett säkert sätt. I detta ingår att

- delta i och stödja IT-säkerhetsarbetet
- ansvara för hur, av vem och vilken information som ska registreras
- ansvara för vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen och hur detta ska ske
- besluta om och beställa enskilda användares behörighet till IT-systemet och svara för användarens kompetens inom systemet
- omgående anmäla till systemansvarig samt IT-support när användare slutar eller av annat skäl ska ha ändrade behörigheter
- verka för att kunskap om IT-säkerhet bibehålls.

2.5 Systemansvarig

Systemansvarig utses av systemägaren och är den som har ansvaret för det dagliga underhållet och användningen av IT-systemet. I detta ingår att

- delta i och stödja IT-säkerhetsarbetet
- verkställa systemägarens beslut
- sköta användar- och behörighetsadministration
- hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till systemägaren för vidare befordran till IT-rådet
- dokumentera uppkomna fel och brister i systemet och rapportera dessa till systemägare
- rapportera avvikelser i systemet via kommunens avvikelserapporteringssystem
- medverka i planering av datum för produktionssättning inför nya releaser/versioner
- medverka i tester vid uppdateringar och felrättningar
- bevaka att systemet hålls uppdaterat med buggfixar och säkerhetsuppdateringar

- upprätta förteckning över förslag till förändringar från användare till systemägaren
- ansvara för användarsupport beträffande verksamhetsrelaterade frågor i systemet
- samverka med IT-funktionen och delta i arbetet med säkerhetsfrågor som rör systemet
- reservrutiner enligt kontinuitetsplaneringen är kända
- medverka i utbildning av systemets användare
- ansvara för uppdatering av grunduppgifter i IT-systemet
- ha kontakt med IT-systemets leverantör i övergripande frågor om krav på systemet
- ha kontakt med leverantörens kundtjänst/support.

2.6 Kontaktperson

Kontaktperson kan vid behov, utifrån systemets omfattning, utses av verksamhetsansvarig. Kontaktpersonen har goda kunskaper om den egna verksamheten och är daglig användare av IT-systemet. Kontaktpersonen är en länk mellan systemansvarig och användarna inom den egna verksamheten. I detta ingår att

- hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till systemansvarig
- delta i och stödja IT-säkerhetsarbetet
- medverka i planering för produktionssättning inför nya releaser/versioner
- medverka i tester vid uppdateringar och felrättningar
- ge support till användarna inom sitt verksamhetsområde
- samverka med systemansvarig i frågor kring IT-systemet
- medverka i utbildning av IT-systemets användare
- ta emot förslag till förändringar i IT-systemet från användare och lämna vidare till systemansvarig
- vid behov (inom sitt verksamhetsområde) hjälpa systemansvarig med behörighets-administration.

2.7 Användare

Varje användare ska följa gällande regler för IT-säkerhet. I detta ansvar ingår att

- delta i och stödja IT-säkerhetsarbetet
- noga ta del av och följa aktuella säkerhetsföreskrifter för användare
- rapportera olika former av fel, brister och avvikelser, t ex misstänkt virusangrepp enligt fastställda rutiner
- föreslå förändringar till verksamhetsansvarig
- påtala egna behov av utbildning

2.8 IT-ansvarig

IT-ansvarig ansvarar för kommunens tekniska IT-infrastruktur och har det övergripande ansvaret för att ett IT-systems tekniska delar fungerar.

IT-ansvarig ansvarar för att

- systemsäkerhetsplan för teknisk IT-infrastruktur upprättas och hålls aktuell
- delta i och stödja IT-säkerhetsarbetet
- efter beställning tilldela och administrera behörigheter till den gemensamma infrastrukturen
- utforma förslag på den strategiskt långsiktiga och övergripande IT-utvecklingen
- omvärldsbevakning sker och avrapporteras regelbundet till IT-rådet

- systemägarens krav enligt systemsäkerhetsplaner omsätts i den tekniska infrastrukturen
- i samråd med systemägare se till att IT-systemet fungerar ihop med andra IT-system
- testmiljö finns tillgänglig vid behov
- rutiner för säkerhetskopiering uppfyller systemägarnas krav
- teknisk infrastruktur – IT-miljön hålls uppdaterad med buggfixar och säkerhetsuppdateringar
- säkerhetskopierat material förvaras på ett betryggande sätt och att det regelbundet kontrolleras att återläsningsrutiner fungerar
- reservrutiner, serviceavtal mm finns så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses
- tillhandahålla teknisk support för användare (”IT-support”)
- biträda systemägarna i avbrottsplaneringen
- vara teknisk rådgivare till systemägarna då förändringar i IT-systemen är aktuella
- arbetsstationer (PC), nätverk och gemensamma resurser har tillräcklig kapacitet (IT-rådet)
- den tekniska infrastrukturens IT-säkerhet motsvarar systemägarnas krav
- ett IT-system håller den tekniska och funktionella kvalitet som överenskommits med systemägaren
- administration av organisationens brandväggar sker och skydd mot skadlig kod finns
- Säkerhetsföreskrifter för drift av IT-system är upprättade och aktuella.

2.9 Systemadministratör

Systemadministratören har den tekniska kompetensen och ansvarar tillsammans med verksamhetsansvarig och systemansvarig för att den dagliga driften upprätthålls. Systemadministratören tillhör IT-enheten och utför arbetet enligt överenskommelse mellan systemägaren och IT-ansvarig.

Systemadministratören har bland annat följande uppgifter:

- tillhandahåller teknisk support till systemansvarig
- deltar och stödjer IT-säkerhetsarbetet
- initierar felsökning vid driftsstörningar och vidtar nödvändiga åtgärder och dokumenterar dessa
- ansvarar för att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs
- ansvarar för systemets tekniska kontinuitetsplan

2.10 IT-support

IT-supporten är kommunens samordnade tekniksupport.

IT-supporten har bland annat följande uppgifter:

- hantera alla typer av fel och incidenter i den tekniska IT-infrastrukturen.
- registrerar/avregistrerar användare i kommunens gemensamma nätverk med de behörigheter som verksamhetsansvarig har beslutat
- registrerar inrapporterade IT-säkerhetsincidenter och rapportera dessa till IT-säkerhetssamordnare.
- för register över aktuell IT-infrastruktur
- informerar om gällande IT-säkerhetsföreskrifter.

2.11 IT-säkerhetssamordnare

IT-säkerhetssamordnare stödjer arbetet med att uppnå målen i riktlinjer för IT-säkerhet Detta kan innebära aktivt deltagande i interna och externa projekt och kontaktnät. Delta i diskussioner kring metoder, plattformar och IT-system. IT-säkerhetssamordnare kan sägas arbeta som konsult åt verksamheten och är i IT-säkerhetsfrågor direkt underställd organisationens ledning. IT-säkerhetssamordnare deltar i samordningen av IT-säkerhetsarbetet inom organisationen och har till uppgift att

- ingå i och rapportera till IT-rådet
- följa upp att riktlinjer för IT-säkerhet och säkerhetsföreskrifter för förvaltning av IT-system och säkerhetsföreskrifter för användare av revideras och hålls aktuella
- stödja IT-ansvarig vid upprättande av kontinuitetsplan för teknisk IT-infrastruktur
- stödja systemägarna vid
  - upprättande av systemsäkerhetsplan
  - upprättande av kontinuitetsplanering för verksamheten
  - säkerhetsgranskning inför driftgodkännande
  - utbildning i IT-säkerhetsfrågor
- sammanställa och rapportera IT-säkerhetsincidenter
- följa upp hur riktlinjer för IT-säkerhet efterlevs och delta i IT-säkerhetsrevisioner

3 IT-SÄKERHETSUTBILDNING

Information och utbildning inom IT-säkerhetsområdet ska ges alla användare och omfatta:

- IT-säkerhetens betydelse för verksamheten
- innehållet i riktlinjer för IT-säkerhet
- tillämpliga delar av innehållet i IT-säkerhetsföreskrifterna för förvaltning, användare och drift av IT-system
- riktlinjer för kommunikation

Nya användare ska i introduktion för nyanställda ges grundläggande IT-säkerhetsutbildning före tilldelning av behörighet i nätverket.

Systemägare ansvarar för att:

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

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

4 SÄRSKILDA RUTINER

4.1 Åtkomst till IT-resurser

För att säkerställa att endast behöriga användare förekommer i IT-systemen ska följande rutiner gälla:

4.1.1 Behörighetsadministration

Beställning, förändring och avslut av åtkomst till IT-systemen ska ske via kommunens intranät av verksamhetsansvarig chef. Upprättat användaravtal ska sparas hos beställaren och respektive systemansvarig enligt dokumenthanteringsplan. Aktuell användare får därefter tillgång till beställda IT-system. Samma förfarande ska användas när konsulter eller andra utför arbete i organisationens IT-system.

Behörighet till IT-system där e-legitimation krävs hanteras enligt särskilda rutiner.

4.1.2 Behörighetskontroll

Leverantörslösenord är hemliga och ska förvaras inlåsta. För att förhindra att de kan användas i IT-systemen ska de vara ändrade. Vid allt arbete i organisationens tekniska infrastruktur ska autentisering ske med smarta kort. IT-enheten ska tillhandahålla kort till externa medarbetare till exempel konsulter.

4.1.3 Loggning och spårbarhet

Systemägarnas krav på säkerhets- och transaktionsloggar ska framgå av respektive systemsäkerhetsplan.

4.1.4 Informationsklassning

Regler för klassning av information ska framgå av säkerhetsföreskrifter för användare av IT-system.

4.1.5 Distansarbete, extern anslutning och mobil datoranvändning

Systemägaren beslutar om ett IT-systems information ska få hanteras på distans med stationär eller mobil utrustning. Allt distansarbete och mobil datoranvändning ska vara reglerat i avtal mellan arbetsgivaren och den anställde enligt särskild rutin.

Regler för extern anslutning och mobil datoranvändning anges i säkerhetsföreskrifterna för användare av IT-system.

4.2 Drift och förvaltning av IT-system

IT-rådet inventerar årligen verksamheternas behov av IT-stöd. Gruppen analyserar och klassificerar behoven inom något av områdena (införande, utveckling, drift eller avveckling) och lämnar förslag till mål för kommande verksamhetsår (om möjligt i prioritetsordning) till kommunchefen för beslut. Förslag kan också avse långsiktiga mål beroende på ärendets karaktär.

Utifrån klassificering utformas projektplaner enligt nedan. Beslutade förändringar ska ingå i budgetarbetet.

4.2.1 Införande och/eller avveckling av IT-system

Vid införande och avveckling av ett IT-system ska verksamhetsansvarig chef/systemägare efter samråd med IT-rådet utforma en projektplan. Denna plan tas fram i samverkan med IT-ansvarig.

4.2.2 Driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett IT-system uppfyller ställda säkerhetskrav enligt systemsäkerhetsplanen.

Systemägaren beslutar om driftgodkännande i samverkan med IT-ansvarig.

4.2.3 Systemförvaltning

Med systemunderhåll avses samtliga aktiviteter som görs för att styra, administrera och verkställa förändringsarbetet av redan existerande IT-system och stödja användandet (ändra, rätta, uppdatera, komplettera med mera).

Med systemutveckling avses större förändringar av IT-system där nya verksamhetsprocesser förs in i befintliga system. Vid beslut om systemutveckling upprättas en projektplan i samverkan med IT-ansvarig.

4.2.4 Drift

Reglerna för systemdrift ska vara samlade i säkerhetsföreskriften för drift av IT-system. Organisationens tekniska IT-infrastruktur ska vara dokumenterad i särskild systemsäkerhetsplan.

4.2.5 IT-incidenthantering

Erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Vid misstanke om intrång eller andra incidenter ska användare agera enligt säkerhetsföreskrifter för användare av IT-system.

IT-rådet ska informeras om:

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

Vid händelser som innebär en svår påfrestning ska kommunens krisledningsorganisation informeras (säkerhetssamordnare eller kommunchef) enligt riktlinjer som anges i lednings- och informationsplanen.

Brott ska anmälas till polismyndigheten.

4.2.6 Tillträdesskydd

IT-ansvarig ska besluta om vilka som ska ha tillträde till dator- och växelrum. För att kunna följa upp detta ska alla besökande vara registrerade.

4.2.7 Säkerhetskopiering och lagring

Systemägarens krav på säkerhetskopiering och lagring för de egna systemen ska framgå av dess systemsäkerhetsplaner. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsplan för IT-infrastrukturen. Upprättade dokument och handlingar ska lagras enligt dokumenthanteringsplan.

4.3 Datakommunikation

4.3.1 Internt

Orust kommuns gemensamma förvaltningsnätverk ska vara dokumenterat i säkerhetsföreskrifter för drift av IT-system.

4.3.2 Externt

Organisationen är för sin verksamhet beroende av datakommunikation via Internet. Denna kommunikation sker dels via upprättade kanaler för specifika system och dels via öppen internet .

Mellan det interna nätverket och externa nätverk ska det finnas en brandvägg som hanteras av systemägaren för den tekniska IT-infrastrukturen.

4.3.3 Brandväggar

Systemägaren ska besluta om:

- vad som ska loggas i brandväggen
- vem som ansvarar för uppföljning av loggar
- hur ofta uppföljning ska ske
- hur länge loggarna ska sparas

4.3.4 Användningen av e-post och Internet

I säkerhetsföreskrifterna för användare av IT-system anges användning av Internet och e-post.

I e-postsystemet ska finnas en loggningsfunktion där inkommande och utgående e-post registreras så att alla meddelanden kan spåras.

5 KONTINUITETSPLANERING

Av kommunens systemsäkerhetsplaner ska framgå de enskilda IT-systemens krav på avbrotts- och katastrofberedskap. Kraven ska vara sammanställda i systemsäkerhetsplanen för den tekniska IT-infrastrukturen.