IT-Säkerhets-instruktion:

- Förvaltning

Arvidsjaurs kommun

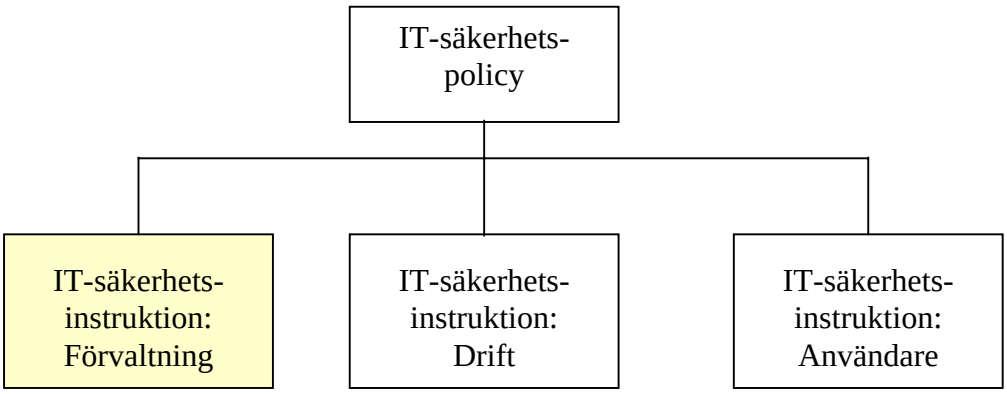
Arvidsjaurs kommun

IT– säkerhetsinstruktion: Förvaltning

1. IT-SÄKERHETSINSTRUKTION FÖRVALTNINGS ROLL I IT-SÄKERHETSARBETET

IT-säkerhet är en del i Arvidsjaurs kommuns lednings- och kvalitetsprocess som skall bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskapsmyndighetens (KBM) rekommendationer om basnivå för IT-säkerhet (BITS) skall gälla som ramverk för IT-säkerhetsarbetet.

Styrande dokument för IT-säkerhetsarbetet är:



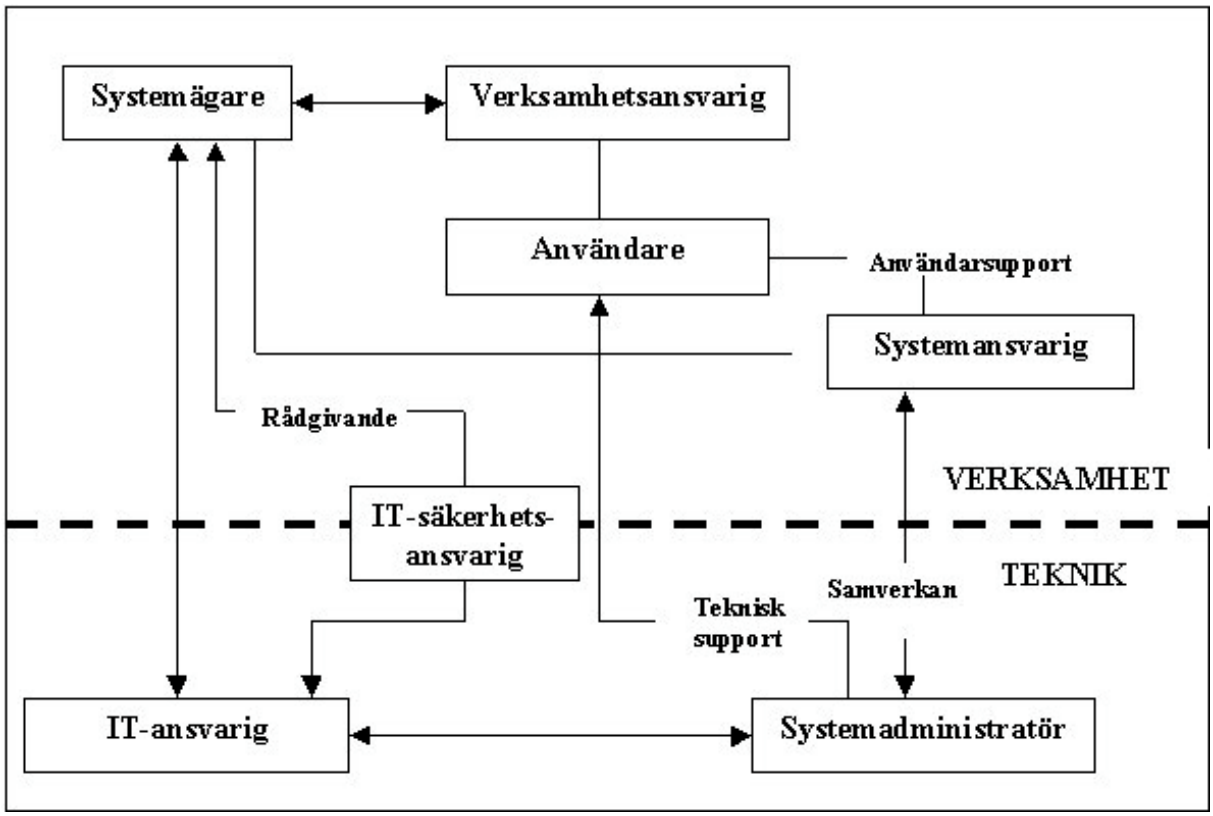
IT-säkerhetspolicy och IT-säkerhetsinstruktioner fastställs av kommunfullmäktige.

IT-säkerhetspolicyn redovisar ledningens viljeinriktning och mål för IT-säkerhetsarbetet. Detta dokument, IT-säkerhetsinstruktion Förvaltning, utgår från IT-säkerhetspolicyn 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 kommunen
- beskriva hur IT-säkerhetsarbetet skall bedrivas.
- ange särskilda riktlinjer som kan vara aktuella

2. ORGANISATION, ROLLER OCH ANSVAR

Den interna kommunen och de roller som ingår i IT-säkerhetsarbetet framgår av nedanstående bild. Omfattningen av det ansvar som vilar på de olika rollerna beskrivs under punkt 2.1 – 2.8.



2.1 ÖVERGRIPANDE ANSVAR

Det övergripande ansvaret för kommunens IT-system vilar på kommunfullmäktige som också utser systemägare för kommunens IT-system.

2.2 IT-BEREDNINGSGRUPPEN

För att uppnå samsyn i IT-frågor skall en IT-beredningsgrupp inrättas. Gruppen har som övergripande uppgift att samordna kommunens långsiktiga IT-behov samt hantera och utreda IT-frågor och förbereda dessa för beslut.

Inför den *årliga verksamhetsplaneringen* skall gruppen i samverkan med enhetscheferna inventera verksamheternas 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 frågor om systemutveckling och systemunderhåll och som omfattar 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)

När inventeringen gjorts analyserar och sammanställer gruppen behoven i form av förslag till årliga mål för kommande verksamhetsår som överlämnas för beslut.
Gruppens uppgifter i övrigt är bl.a. att:

- under pågående verksamhetsår samverka med enhetscheferna omkring frågor och uppdrag som uppstår inom ovanstående områden (t.ex. akuta behov, inkomna förslag m.m.)
- omvärldsbevakning sker
- delta i utformningen av kontinuitetsplanen
- planera för hur IT-säkerhetsfrågor från genomförda risk- och sårbarhetsanalyser skall hanteras
- samordna systemägarnas krav på den IT-tekniska infrastrukturen (krav från dessas systemsäkerhetsplaner)
- samordna att avtal med annan part som utför tjänst eller uppdrag beaktar de informationssäkerhetskrav som KBM ställer
- samordna kompetensutveckling hos verksamhetsansvariga inom områdena IT, juridik och kvalitet

2.3 SYSTEMÄGARE

Systemägaren, nämnd etc., utses av kommunfullmäktige och ansvarar för att egna IT-system förvaltas på för verksamheten bästa sätt. Systemägaren fattar de avgörande besluten om IT-systemet inom ramen för resurstilldelningen för sin verksamhet.

Systemägaren, som också är informationsägare och registeransvarig, ansvarar för informationen i de IT-system som används i den egna verksamheten samt för att denna information hanteras på ett ur säkerhetssynpunkt tillfredsställande sätt.

2.4 VERKSAMHETSANSVARIG CHEF

Verksamhetsansvarig chef har ansvar för bl.a.:

- att inför den årliga verksamhetsplaneringen, initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-beredningsgruppen i form av kortfattade, översiktliga mål och krav inom områdena införande, systemförvaltning, drift och avveckling
- att löpande följa upp att egna system stödjer verksamheten
- att bevaka förändringar i eller som påverkar verksamheten
- att delta i IT-säkerhetsarbetet för de egna systemen
- att fastställa ansvar och roller för respektive system (t.ex. systemförvaltare, styrgrupp)
- att nödvändiga licenser och tillstånd finns
- att med stöd av KBM:s IT-säkerhetsguide upprätta *systemsäkerhetsplaner* för de egna IT-systemen
- att driftgodkänna IT-systemet
- att besluta om hur media med sekretessbelagd information skall avvecklas
- vilket informationsinnehåll aktuellt IT-system skall ha
- vilka uppgifter som skall tillhandahållas enligt offentlighetsprincipen och hur detta skall ske
- att skriftligt beställa enskilda användares behörighet till IT-systemet
- hur och av vilka informationen skall registreras i systemet

För att säkerställa att endast behöriga användare använder systemet skall verksamhetsansvarig chef anmäla till systemansvarig och IT-avdelning när personal slutar eller av annat skäl skall ha ändrade behörigheter.

(Se även kap 3 som beskriver kommunens rutiner inom områden införande, förvaltning, drift och avveckling)

2.5 SYSTEMANSVARIG

Systemansvarig utses av systemägare och ansvarar för den dagliga användningen av IT-systemet. Systemansvarig verkar för att säkerställa en säker och rationell drift.
Systemansvarig ansvarar för bl.a.:

- att verkställa systemägarens beslut
- att delta i IT-säkerhetsarbetet
- att sköta användar- och behörighetsadministration.
- att hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till verksamhetsansvarig chef för vidare befordran till IT-beredningsgruppen (omvärldsbevakning)
- att dokumentera uppkomna fel, brister och incidenter i systemet och rapportera dessa till verksamhetsansvarig chef och IT-ansvarig
- att medverka i planering av datum för produktionssättning inför nya releaser/versioner
- att medverka i tester vid uppdateringar och felrättningar
- att bevaka att systemet hålls uppdaterat med buggfixar och säkerhetsuppdateringar.
- att upprätta förteckning över förslag till förändringar från användare till systemägaren
- att ansvara för användarsupport beträffande frågor om systemets funktioner och användning
- att reservrutiner enligt kontinuitetsplaneringen är kända
- att medverka i utbildning av systemets användare
- med stöd av KBM:s IT-säkerhetsguide upprätta *systemsäkerhetsplaner* för de egna IT-systemen

2.6 IT-ANSVARIG

Ansvarig för IT-system är systemägare för kommunens IT-infrastruktur d.v.s. nät och servrar m.m. och har det övergripande ansvaret för att ett systems tekniska delar fungerar.

Ansvarig för IT-system ansvarar för bl.a.:

- att systemsäkerhetsplan för IT-teknisk infrastruktur upprättas och hålls aktuell
- att delta i IT-säkerhetsarbetet
- att efter beställning tilldela och administrera behörigheter till den gemensamma infrastrukturen.
- utformning av förslag på den långsiktiga strategiska IT-utvecklingen
- att omvärldsbevakning sker och avrapporteras regelbundet till IT-beredningsgruppen
- att systemägares krav enligt systemsäkerhetsplaner tillgodoses i den tekniska infrastrukturen
- att i samråd med systemansvariga se till att systemet fungerar ihop med samverkande IT-system
- att testmiljö finns tillgänglig vid behov
- att rutiner för säkerhetskopiering uppfyller systemägarnas krav
- att IT-teknisk infrastruktur hålls uppdaterad med buggfixar och säkerhetsuppdateringar.
- att säkerhetskopierat material förvaras på ett betryggande sätt och att det regelbundet kontrolleras att återläsningsrutiner fungerar
- att reservrutiner, serviceavtal m.m. finns så att verksamhetsansvarig chefs krav på längsta tillåtna avbrottstid kan tillgodoses
- att tillhandahålla teknisk support för användare (Helpdesk)

- att biträda systemägarna i avbrottsplaneringen
- att vara teknisk rådgivare till verksamhetsansvarig chef då förändringar i systemen är aktuella
- att arbetsstationer (PC), nätverk och gemensamma resurser har tillräcklig kapacitet
- att den IT-tekniska infrastrukturens säkerhet motsvarar systemägarnas krav
- administration av myndighetens brandväggar och skydd mot skadlig kod
- att IT-säkerhetsinstruktion: Drift är aktuell

IT-ansvarig ansvarar för bl.a.:
- framtagande och revidering av IT-säkerhetspolicy med tillhörande säkerhetsinstruktioner
- att följa upp att de krav på IT-säkerhet som fastställts i IT-säkerhetspolicy och instruktioner efterlevs
- vid behov lämna förslag till säkerhetshöjande åtgärder

I IT-ansvarigs uppgift ingår också att:
- genomföra enhetsbesök (informera och utbilda samtliga anställda i IT-säkerhetsfrågor)
- stödja systemägarna vid
    - upprättande av systemsäkerhetsplan
    - upprättande av IT-säkerhetsinstruktioner
    - kontinuitetsplanering för dennes IT-system (vid behov)
    - säkerhetsgranskning inför driftgodkännande
- sammanställa och rapportera IT-säkerhetsincidenter internt och till PTS
- ansvara för upprättande och underhåll av KBM:s systemförteckning
- ansvara för upprättande av kontinuitetsplan för IT-infrastruktur
- omvärldsbevakning

2.7 IT-AVDELNINGENS SYSTEMADMINISTRATÖRER
Ansvarig för IT-system utser en av dessa till systemförvaltare för IT-infrastrukturen. Övriga systemadministratörer ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-ansvarig.

Systemadministratören har bl.a. följande uppgifter:
- registrera/avregistrera användare i systemet (infrastrukturen) med de behörigheter eller den behörighetsprofil som systemägaren har beslutat
- tillhandahålla teknisk support
- delta i IT-säkerhetsarbetet
- initiera felsökning vid driftsstörningar, vidta nödvändiga åtgärder och dokumentera dessa
- ansvara för att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs

2.8 ANVÄNDARE
Varje användare skall följa gällande regler för IT-säkerhet. I detta ansvar ingår att:
- ta del av och följa aktuella IT-säkerhetsinstruktioner
- föreslå förändringar till respektive chef
- påtala egna behov av utbildning till respektive chef

2.9 IT-SÄKERHETSANSVARIG

IT-säkerhetsansvarig stödjer arbetet med att uppnå IT-säkerhetspolicyns mål. Detta kan innebära aktivt deltagande i projekt, etablerande av interna och externa kontaktnät, utvärdering och deltagande i diskussioner kring metoder, plattformar eller IT-system. IT-säkerhetsansvarig kan sägas arbeta som konsult åt verksamheten.

3. REGLER OCH RUTINER FÖR VISSA OMRÅDEN

3.1 BEHÖRIGHETSADMINISTRATION

Verksamhetsansvarig chef skall beställa behörighet för varje enskild användare på särskild blankett. Verksamhetsansvarig chefs krav på behörighetsadministration skall framgå av de systemsäkerhetsplaner som har upprättats.

3.2 LOGGNING OCH SPÅRBARHET

Krav på säkerhets- och transaktionsloggar skall framgå av de systemsäkerhetsplaner som upprättats.

3.3 KRYPTERING

Kryptering skall användas vid åtkomst av det interna nätet från externa nät.

3.4 DRIFT OCH FÖRVALTNING AV IT-SYSTEM

Inför den årliga verksamhetsplaneringen inventerar IT-beredningsgruppen verksamheternas behov av IT-stöd. Gruppen analyserar och klassificerar dessa inom något av områdena införande, systemförvaltning, drift eller avveckling och lämnar förslag på årliga mål för kommande verksamhetsår (om möjligt i prioritetsordning) till kommunstyrelsens budgetberedning. Förslag kan också avse långsiktiga mål beroende på ärendets karaktär.

När beslut har fattats förtydligar IT-beredningsgruppen dessa i form av riktlinjer och anvisningar för hur de skall förverkligas. Utifrån klassificering utformas dessa i projektplaner enligt nedan.

3.4.1 INFÖRANDE AV IT-SYSTEM

Vid införande av IT-system skall verksamhetsansvarig chef i samråd med IT-beredningsgruppen utforma en projektplan för införandet. Denna plan skall omfatta följande:

- verksamhetens beskrivning av behov och mål med anskaffningen
- lönsamhetskalkyl
- en inledande risk- och sårbarhetsbedömning (Stöd av KBM:s IT-säkerhetsguide)
  Den inledande risk- och sårbarhetsbedömningen är ett viktigt underlag för den kravspecifikation som skall upprättas och syftar bl. a. till att klarlägga de säkerhetskrav som verksamhetens ställer i form av:
  - krav på säkerhet avseende sekretess, riktighet och tillgänglighet
  - rättsliga, -verksamhets-, och hotrelaterade krav
  - kommunikationsberoende (internt och externt)
  - reservrutiner m.m..
- Kravspecifikation
  Kraven från risk- och sårbarhetsbedömningen utökas med bl.a.:
  - krav med anledning av integration med andra system
  - krav vid införande
  - krav på test och acceptans
  - ytterligare krav som skall gälla fram till den tidpunkt då den tilltänkte systemägaren övertar ansvaret och systemet övergår till normal systemförvaltning m.m. i den kravspecifikation som skall utgöra grunden för upphandlingen
  - tidplan
  - resurser (personella och ekonomiska)

- när och hur uppföljning, utvärdering och avrapportering skall ske
- när och hur medarbetarna skall informeras och utbildas

- Upphandling
  - en upphandling görs med beaktande av lagen om offentlig upphandling
  - tillämpliga ramavtal skall användas
  - om möjligt skall standardprodukter användas

- Inför drift och förvaltning

  Ansvarig för nyanskaffningsprojekt förbereder överlämnandet från test och utveckling till drift och förvaltning tillsammans med den tilltänkte systemägaren. Beslut om tidpunkt från vilken systemet övergår från projekt till förvaltning fattas av systemägaren. I och med detta övergår ansvaret till systemägaren som då också övertar all dokumentation.

3.4.2 Systemutveckling och systemunderhåll (Systemförvaltning)

Med systemutveckling avses samtliga aktiviteter som görs för att styra, administrera och verkställa förändringsarbetet av redan existerande objekt och stödja användandet (utveckla, ändra, rätta, uppdatera, komplettera m.m.)

Målet med systemets förvaltning är beroende av målen med verksamheten och sätts vid verksamhetsplaneringen. Målen med systemförvaltningen sätts av verksamhetsansvarig chef i samråd med IT-beredningsgrupp. Förslag till årliga mål utarbetas av verksamhetsansvarig chef i samråd med IT-beredningsgruppen.

Vid beslut om systemförvaltning upprättas en projektplan som skall omfatta:

- tidplan
- resurser (personella och ekonomiska)
- när och hur uppföljning, utvärdering och avrapportering skall ske
- när och hur medarbetarna skall informeras och utbildas
- målformulering
- budget

  - verksamhetsansvarig chef ansvarar för systemets ekonomi inom ramen för ledningens resurstilldelning.
  - för att kunna följa kostnadsutvecklingen på ett effektivt sätt upprättar verksamhetsansvarig chef, i samråd med IT-beredningsgruppen, en systemförvaltningsbudget som omfattar en utvecklings- och en driftbudget. Dessa upprättas inför verksamhetsplaneringen.

- Initiering av förändringsförslag
  Förslag om önskemål på förändringar i systemet lämnas till verksamhetsansvarige för vidare befordran till systemägaren och IT-beredningsgruppen.

- Mottagning av förändringsförslag
  IT-beredningsgruppen och verksamhetsansvarig chef skall först avgöra prioritet för ändringsförslaget enligt följande:

  Omedelbar åtgärd
  Fel som kräver omedelbar åtgärd och som inte är inplanerade. En akut förändring får alltid högsta prioritet. Vid akuta fel informerar systemadministratören alltid systemägaren. Systemadministratören ansvarar för att felet åtgärdas. Även akuta åtgärder skall dokumenteras och arkiveras.

  Åtgärd som kan inplaneras:
  Utvecklingsåtgärd planeras in på vanligt sätt av systemägare, IT-beredningsgrupp och leverantör. Medel finns avsatta i utvecklingsbudgeten för året.

  Driftåtgärd planeras in på vanligt sätt av systemägare, IT-beredningsgrupp och leverantör. Medel finns avsatta i driftbudgeten för året.

  Därefter inordnas förändringsförslagen i någon av följande klasser:

Rättning	▪ Identifiering av fel i systemet
Anpassning	▪ Förändring i systemet som finns beroende på förändring i infrastrukturen ▪ Förändring av systemet beroende på ändringar i lagar och förordningar ▪ Förändring i systemet beroende på nya säkerhetskrav
Förbättring	▪ Felrättningar ▪ Identifiering av brister i systemet ▪ Önskemål om förbättringar ▪ Förändring av verksamheten som påverkar systemet
Sanering/ Avveckling	▪ Rensning i databas ▪ Systemet behövs inte längre för att stödja verksamheten

- Förberedelse
  Alla åtgärdsförslag med prioriteringsklass *åtgärd som kan inplaneras* förbereder verksamhetsansvarig chef och IT-beredningsgruppen. Det huvudsakliga arbetsinnehållet i förberedelse-arbetet är att komplettera med nödvändig information för beslut, samt göra en bedömning om den önskade ändringen är möjlig att genomföra

  När information om systemets funktionella och tekniska krav är framtaget så måste det även göras en konsekvensbedömning om vad förändringen innebär i integration med förändringen i systemet samt en tid- och kostnadskalkyl.

  Med informationen som underlag tar IT-beredningsgruppen ställning till ändringsförslaget. Är förslaget orealistiskt av t.ex. tids-, kostnads- eller kompetensskäl skrivs det in som motivering och förslagsgivaren informeras. Även detta förslag dokumenteras och aktiveras.

- Prioritering
  Förändringsförslagen rangordnas slutligen. Prioriteringen är dynamisk. Det kan alltså innebära att omprioriteringar blir aktuella om förutsättningarna vid prioriteringstillfället ändras eller om systemägaren vill det. Vid större omprioriteringar skall alltid systemägaren informeras.

- Beställning
  IT-beredningsgruppen ansvarar för att alla ändringsförslag som är beslutade i samverkan med systemägaren blir åtgärdade. Beställning bör sedan ske efter att man tagit ställning till upphandlingsform. Beställningen dokumenteras. Behov av förvaltningsåtgärder som inte ryms i den disponibla förvaltningsbudgeten kan endast systemägaren besluta om. Dessa förvaltningsåtgärder skall dock först beredas av IT-beredningsgruppen och sedan kostnadsbedömas tillsammans med leverantören.

- Ändring och test
  För genomförandet av ändring och test ansvarar leverantören. Ändringarna kan inkludera även anpassning av system-, drift och användardokumentation beroende på vad som avtalats. Det är viktigt att dokumentationen är aktuell oavsett vem som genomför ändringarna. Alla förändringar och testresultat bör bifogas. Under själva ändrings- och testfasen skall kontinuerliga möten hållas med leverantör och projektgrupp för att stämma av framåtskridandet och eventuella problem.

- Acceptans
  IT-beredningsgruppen ansvarar för att test sker av levererad produkt. Vilken testambition som IT-beredningsgruppen har kan t.ex. vara beroende av förändringens storlek, komplexitet eller av leverantören bifogat testprotokoll. Eventuella kriterier för godkännande och testfall prövas av IT-beredningsgruppen och resultatet dokumenteras. Om leveransen och dess resultat godkänns meddelas leverantören detta. Om leveransen och dess innehåll inte godkänns skall leverantören åtgärda felen och återkomma med ny tid för leverans.

3.4.3 Drift

Möjligheten till en säker och ändamålsenlig drift av ett IT-system är beroende av helhetstäckande och aktuell dokumentation. Myndighetens regler för systemdrift skall vara samlade i IT-säkerhetsinstruktion Drift och innehålla bl. a:

- systemdokumentationer
- driftdokumentationer
- bemanningsplan (nyckelpersonberoende)
- tillträdes- och brandskydd
- elförsörjning
- regler för säkerhetskopiering
- regler för förvaring av datamedia

Kommunens IT-tekniska infrastruktur skall vara dokumenterad i särskild systemsäkerhetsplan.

3.4.4 Avveckling av IT-system

IT-system som inte längre behövs för verksamheten skall avvecklas snarast.

Verksamhetsansvarig chef skall efter samråd med IT-beredningsgruppen besluta om och när ett IT-system skall avvecklas. En plan för avvecklingen skall upprättas. Planen skall särskilt beakta:

- rättsliga regler såsom Arkivlagen, Personuppgiftslagen (PUL)
- vad som skall tas ut ur systemet före avveckling (på papper eller media)
- om systemet innehåller ärenden vilka behöver avslutas i diariet
- om återläsning av innehåll behöver kunna ske längre fram
- om uppgifter behöver flyttas över till annat IT-system
- destruktion av media som innehållit information (rutinen ej klarlagd)

3.5 INCIDENTHANTERING

Följande rutin gäller vid incidenter eller misstanke om sådana:
- användare agerar enligt vad som framgår av IT-*säkerhetsinstruktion: Användare*
- personal vid datadriften agerar enligt vad som framgår av *IT-säkerhetsinstruktion: Drift*

Ansvaret för uppföljning av incidenter åvilar IT-säkerhetsansvarig.
Detta innebär att incidenterna skall:
- sammanställs och rapporteras till ledningen
- rapporteras till Post- och telestyrelsen (PTS)

Uppföljningsarbetet innebär bl.a. att belysa följande:
- vad som möjliggjorde att incidenten inträffade
- konsekvenser som incidenten medförde
- erfarenheter av det inträffade
- förebyggande åtgärder som kan vara aktuella

IT-säkerhetsansvarig ansvarar för att eventuella beslut om ytterligare säkerhetsåtgärder tas och att dessa genomförs.

3.6 TILLTRÄDESSKYDD

IT-ansvarig skall besluta om vilka som skall ha tillträde till serverrum.

3.7 SÄKERHETSKOPIERING OCH LAGRING

Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen skall framgå av de systemsäkerhetsplaner som upprättats. Kraven i dessa planer skall vara koordinerade i systemsäkerhetsplanen för IT-infrastrukturen.

3.8 EXTERNA ANSLUTNINGAR

Verksamhetsansvarig chef och IT-avdelningen skall ta ställning till hur användaridentifiering skall ske vid externa anslutningar.

3.9 BRANDVÄGGAR

Systemägarna skall besluta om:
- vad som skall loggas i brandväggen
- vem som ansvarar för uppföljning av loggar
- hur ofta uppföljning skall ske
- hur länge loggarna skall sparas

3.10 DISTANSARBETE M.M.
Arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket är normalt inte tillåtet. Handdatorer, digitala kameror, mobiltelefoner m.m. får inte anslutas till datorer som inte har ett uppdaterat virusprogram. All kringutrustning skall vara godkänd och installerad av IT-avdelningen.

3.11 INTERNET
Loggning skall ske av Internettrafiken för att möjliggöra spårning av intrång och missbruk. Riktlinjer i övrigt framgår av säkerhetsinstruktion Användare.

3.12 E-POST
I e-postsystemet skall finnas en loggningsfunktion där inkommande och utgående e-post registreras så att alla meddelanden kan spåras. Riktlinjer i övrigt framgår av säkerhetsinstruktion Användare.

4. IT-SÄKERHETSUTBILDNING

IT-säkerhetsansvarig ansvarar för att alla medarbetare skall ges information och utbildning inom IT-säkerhetsområdet, detta skall omfatta:

- IT-säkerhetens betydelse för verksamheten
- innehållet i kommunens IT-säkerhetspolicy
- tillämpliga delar av innehållet i IT-säkerhetsinstruktionerna Förvaltning, Användare och Drift

Nya medarbetare skall ges grundläggande säkerhetsutbildning före tilldelning av behörighet i nätverket.
Verksamhetsansvarig chef ansvarar för att:

- egna medarbetarna erhåller information och utbildning om det centrala innehållet i de systemsäkerhetsplaner de är berörda av
- 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 hos respektive chef.

5. KONTINUITETSPLANERING

Systemägarnas krav på avbrotts- och katastrofplanering skall vara samordnade i kommunens gemensamma kontinuitetsplan. Se IT-säkerhetsinstruktion Drift.

6. DRIFTGODKÄNNANDE

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

Verksamhetsansvarig chef skall besluta om driftgodkännande. Beslutet skall baseras på en granskning och säkerhetsutvärdering som bygger på jämförelse mellan verksamheternas krav och vidtagna säkerhetsåtgärder. Driftgodkännandeprocessen relateras till aktuell systemsäkerhetsplan och skall omfatta:

- avgränsningar
- granskning av säkerhetsåtgärder i IT-systemet
- utvärdering av granskningen i förhållande till systemsäkerhetsplanens krav
- redovisning av beslutsunderlag samt
- beslut

Beslutsunderlaget skall innehålla en sammanfattning av förslag till beslut som kan vara att:

- driftgodkänna IT-systemet
- driftgodkänna IT-systemet efter beslut om när kompletterande säkerhetsåtgärder skall vara genomförda
- inte driftgodkänna IT-systemet.

7. REVIDERING OCH UPPFÖLJNING

Uppföljning är en viktig del i IT-säkerhetsarbetet och skall skötas av verksamhetsansvarig chef, nämnd och revisorer.

Uppföljningen skall bevaka
- att beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- att riktlinjer följs
- att systemsäkerhetsplaner och policydokument vid behov revideras