IT-Säkerhetsinstruktioner: Förvaltning

HÄLLEFORS KOMMUN
Postadress
IT-enheten
712 83 Hällefors

E-post
kommun@hellefors.se
Besöksadress
Sikforsvägen 15
Hällefors

Telefon
0591-641 00 vx

Organisationsnr
212000-1942
Fax
0591-109 76

Bankgiro
193-8950

PlusGiro
11808-3

Innehåll

1 Målsättning

IT-säkerhetsinstruktion Förvaltnings roll i IT-säkerhetsarbetet
IT-säkerhet är en del i Hällefors kommuns lednings- och kvalitetsprocess som ska bidra till att ett IT-system kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskaps-myndighetens rekommendationer om basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet.
BITS – den säkerhetsnivå, som minst måste uppnås för ett IT-system, som bedöms nödvändigt, för att upprätthålla en viss verksamhets basförmåga.

2 Syfte

Styrande dokument för IT-säkerhetsarbetet är:

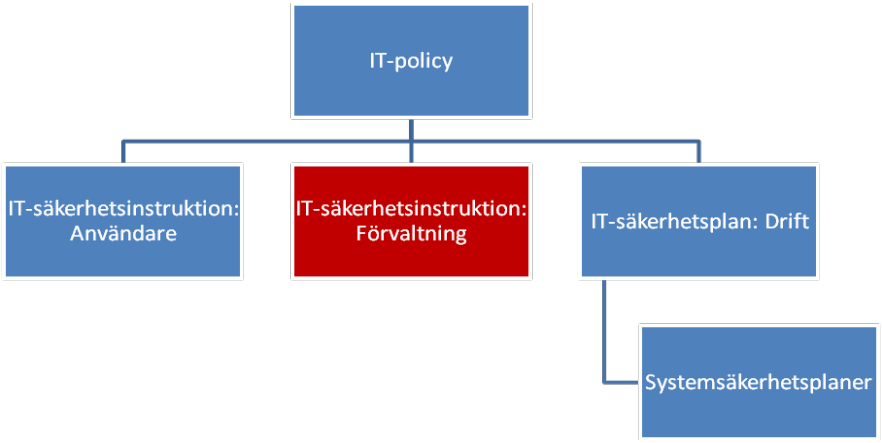

Bild 1 Styrande dokument

IT-policy fastställs av kommunfullmäktige.
IT-säkerhetsinstruktioner fastställs av kommunstyrelsen.

IT-policyn redovisar ledningens viljeinriktning och mål för IT-säkerhetsarbetet. Detta dokument, IT-säkerhetsinstruktion Förvaltning, utgår från IT-policyn 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 särskilda riktlinjer som kan vara aktuella.
- Ligga till grund för framtagande och revidering av systemsäkerhetsplanerna.

3 Ansvarsfördelning

Organisation, roller och ansvar
Ansvaret för informationssäkerheten ska följa linjeorganisationen för varje enskilt IT-system. Förvaltningschefen är i regel systemägare och ansvarig för IT-system som stödjer den egna verksamheten. IT-ansvarig är systemägaren för kommunens tekniska IT-infrastruktur.

Ett IT-system, med alla dess delar, är en resurs i en verksamhet 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 IT-policyns mål.

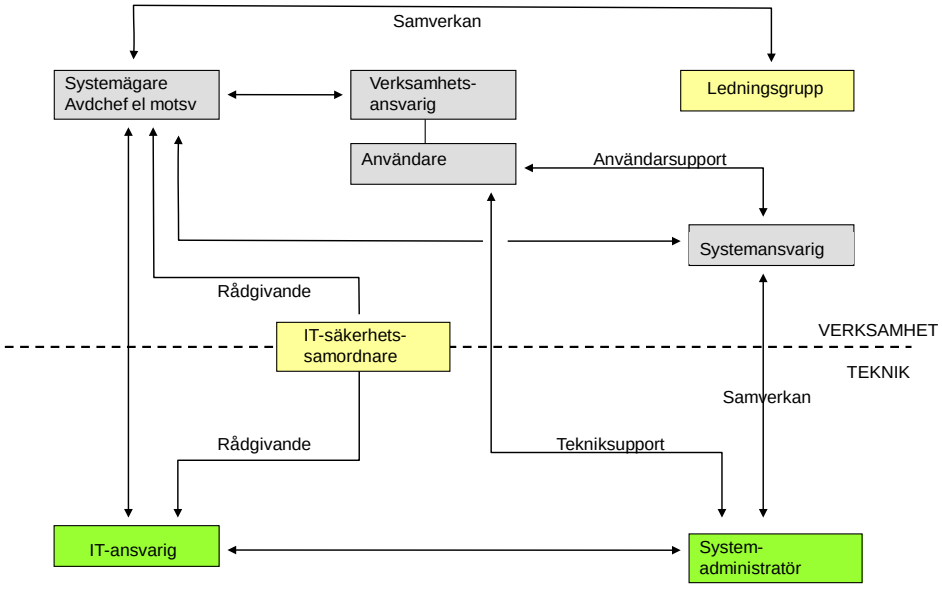

Bild 2 Roller inom IT-säkerhetsområdet

Övergripande ansvar

Det övergripande ansvaret för kommunens IT-system vilar på kommunchefen. Kommunchefen utser systemägare för respektive förvaltnings IT-system.

Kommunförvaltningens ledningsgrupp

För att uppnå samsyn behandlas övergripande IT-frågor av kommunförvaltningens ledningsgrupp. Gruppen skall, hantera och utreda IT-frågor och förbereda dessa för beslut. Kommunchefen leder ledningsgruppen.

Inför verksamhetsplaneringen ska gruppen i samverkan med verksamhetsledarna 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 verksamhetsledarna omkring frågor och uppdrag som uppstår inom ovanstående områden (t.ex. akuta behov, inkomna förslag)
- Omvärldsbevakning sker.
- Delta i utformningen av kontinuitetsplanen.
- Planera för hur IT-säkerhetsfrågor från genomförda risk- och sårbarhetsanalyser ska hanteras.
- Samordna systemägarnas krav på den IT-tekniska infrastrukturen. (krav från deras systemsäkerhetsplaner)
- Samordna att avtal med annan part som utför tjänst eller uppdrag beaktar de informationssäkerhetskrav som IT-policyn ställer.
- Samordna kompetensutveckling hos verksamhetsansvariga inom områdena IT, juridik och kvalitet.
- Ansvara för underhåll av Hällefors kommuns IT-policy och IT-säkerhetsinstruktioner.
- Ansvara för upprättande och underhåll av kommunens systemförteckning.

Systemägare
Systemägaren ansvarar inför ledningen för att egna IT-system förvaltas på för verksamheten bästa sätt. Vid nyutveckling eller större förändringar av IT-system ska systemägaren alltid samråda med IT-ansvarig på ett tidigt stadium. Systemägaren fattar de avgörande besluten om IT-systemets införande, förvaltning, drift och avveckling.

Systemägaren har ansvar för bl.a. följande inom ramen för ledningens resurstilldelning:

- Att inför den årliga verksamhetsplaneringen, initiera och föreslå den egna verksamhetens behov av IT-stöd till kommunförvaltningens ledningsgrupp. (i form av kortfattade och översiktliga mål och krav)
- Att löpande följa upp att egna system stödjer verksamheten.
- Att delta i och stödja IT-säkerhetsarbetet.
- Att en systemsäkerhetsplan upprättas.
- Att i systemsäkerhetsplanen fastställa eventuella tilläggskrav utöver basnivån för IT-systemet utgående från.
- Den information IT-systemet hanterar.
- Lagar, förordningar och författningar.
- Verksamhetens krav på säkerhet vad avser sekretess, riktighet och tillgänglighet.
- Hotbilden mot informationen.
- Vilka olika behörighetsprofiler som skall gälla.
- Omfattning av loggning. (trans- och säkerhetsloggar)
- Hur loggar skall följas upp, arkiveras, förvaras och sparas.
- Längsta acceptabla tid för driftavbrott och/eller informationsbortfall.

- Tid för hur snabbt återläsning av säkerhetskopierat material ska kunna ske.
- Organisation och befattningar som rör systemet t.ex. styrgrupp, verksamhetsansvarig och systemansvarig.

Verksamhetsansvariga
Verksamhetsansvarig utses av systemägare och ansvarar för den dagliga användningen av IT-systemet och för att säkerställa en säker och rationell drift.

Verksamhetsansvarig ansvarar för informationen inom sitt verksamhetsområde och därmed också för informationen i de IT-system som användas i verksamheten samt för att denna information hanteras på ett ur säkerhetssynpunkt tillfredsställande sätt. I detta ingår:

- Att delta i och stödja IT-säkerhetsarbetet.
- Att ansvara för hur, av vem och vilken information som skall registreras. (registeransvarig)
- Att ansvara för vilka uppgifter som skall tillhandahållas enligt offentlighetsprincipen och hur detta skall ske.
- Att besluta om och beställa (skriftligt) enskilda användares behörighet till IT-systemet.
- Att besluta hur och av vem/vilka informationen skall registreras i systemet
- Att anmäla till systemansvarig när personal slutar eller av annat skäl skall ha ändrade behörigheter.
- Att besluta om vilka delar i informationen som är sekretessbelagda.
- Att anmäla till systemförvaltare när personal slutar eller av annat skäl ska ha ändrade behörigheter.

Systemförvaltare
Systemförvaltare utses av systemägare och ansvarar för den dagliga användningen av IT-systemet. Systemförvaltaren samverkar med systemadministratören för att säkerställa en säker och rationell drift. Systemförvaltaren ansvarar för bl.a.:

- Att verkställa systemägarens beslut.
- Att delta i IT-säkerhetsarbetet.
- Att anmäla till systemadministratören när personal slutar eller av annat skäl ska ha ändrade behörigheter.
- Att sköta användar- och behörighetsadministration.
- Att hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till systemägaren för vidare befordran till IT-beredningsgruppen. (omvärldsbevakning)
- Att dokumentera uppkomna fel, brister och incidenter i systemet och rapportera dessa till systemägaren, systemadministratören och IT-säkerhetssamordnare
- 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.

IT-chef
Chef för IT-enheten 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.

Chef IT-enheten 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.
- Attformning 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 systemägare 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 mm finns så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses.
- Att tillhandahålla teknisk support för användare (”helpdesk”).
- Att biträda systemägarna i avbrottsplaneringen.
- Att vara teknisk rådgivare till systemägarna 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 kommunens brandväggar och skydd mot skadlig.
- Att IT-säkerhetsinstruktion: Drift är aktuell.

Systemadministratörer
Systemadministratörerna utses inom verksamheten. Om inte detta är möjligt kan personal från IT-enheten vara systemadministratör. IT-chefen utser en från IT-enheten 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-chef.

- 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.

IT-säkerhetssamordnare
IT-säkerhetssamordnaren stödjer arbetet med att uppnå IT-strategins 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-säkerhetssamordnaren kan sägas arbeta som konsult åt verksamheten och är i IT-säkerhetsfrågor direkt underställd kommunchefen. IT-säkerhetssamordnaren samordnar IT-säkerhetsarbetet inom kommunen och har till uppgift att:

- Följa upp att IT-policyn och IT-säkerhetsinstruktionerna revideras och hålls aktuella.
- Vara rådgivande i IT-säkerhetsfrågor.
- Stödja systemägarna vid:
- Upprättande av systemsäkerhetsplan
- Stödja IT-ansvarig vid upprättande av kontinuitetsplan för teknisk IT- infrastruktur.
- Upprättande av IT-säkerhetsinstruktioner.
- Upprättande av kontinuitetsplanering för verksamheten.
- Säkerhetsgranskning inför driftgodkännande.
- Utbildning i IT-säkerhetsfrågor.
- Sammanställa och rapportera IT-säkerhetsincidenter.
- Följa upp hur IT-policyn efterlevs och delta i IT-säkerhetsrevisioner.

4 Särskilda rutiner

Behörighetsadministration
För att säkerställa att kommunens medarbetare har tillgång till endast den information och de IT-system de behöver för sitt arbete och med rätt behörigheter ska verksamhetsansvarig chef beställa behörigheter för de egna medarbetarna på särskild blankett som tillhandahålls av och återsänds till IT-enheten. Blanketten ska också användas för hantering av behörighet för användare som slutar eller byter arbetsuppgifter. Kopia ska sparas på den egna enheten. Blanketter finns på kommunens Intranät

Loggning och spårbarhet
I samtliga IT-system ska finnas 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. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsplanen för IT-infrastrukturen.

Distansarbete, extern anslutning och mobil datoranvändning
Verksamhetsansvarig chef ska besluta om ett IT-systems information ska få hanteras på distans med stationär eller mobil utrustning i samråd med IT-ansvarig. Distansarbete ska vara reglerat i avtal mellan kommunen och den anställde. För annan extern anslutning och mobil datoranvändning ska särskilda riktlinjer finnas.
Avtalet och säkerhetsinstruktionen ska minst reglera:

- Fysiskt skydd i eller utanför hemmet. (stöldrisk)
- Logiskt skydd. (otillbörlig användning)
- Om utrustningen endast får användas för arbetsgivarens arbete. (virussmitta o.dyl.)
- Hantering av utskrifter. (obehörig tillgång)
- Om lagring och säkerhetskopiering av information ska ske i egen dator eller hos arbetsgivaren. (stöldrisk, obehörig tillgång och förstörelse m.m.)
- Hur eventuella hjälpinsatser utifrån (remote) ska ske. (obehörigt intrång)
- Kontroll av skadlig programkod. (virussmitta o.dyl.)
- Om kryptering krävs vid överföring i vissa fall. (obehörig tillgång och förändring)
- Autenticering vid uppkoppling mot arbetsgivarens nätverk. (obehörig tillgång och förändring).
- Regler hur sekretessmaterial hanteras.

Vid distansarbetsplats ska kommunen tillhandahålla utrustningen. Endast kommunens utrustning får anslutas mot kommunens nätverk och får inte utan särskilt tillstånd anslutas mot andra nätverk eller direkt mot Internetoperatör.

Användning av trådlös anslutning kräver särskilda säkerhetsåtgärder och särskilt tillstånd.

Regler för åtkomst till E-post eller annan information på nätverket från Internet ska framgå av IT-säkerhetsinstruktion: *Användare.*

Drift och förvaltning av IT-system
Kommunens arbetssätt med drift- och förvaltningsfrågor framgår under punkt *3. Ansvarsfördelning* ovan. Följande rutiner ska gälla inom de 4 områdena:

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

- Verksamhetens beskrivning av behov och mål med anskaffningen.
- En inledande risk- och sårbarhetsbedömning. (stöd av KBM:s IT-säkerhetsguide)

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:
- Integrationskrav 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 att 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 ska 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. Om systemet bedöms som samhällsviktigt skall dessutom en systemsäkerhetsplan upprättas.

Systemunderhåll

Med systemförvaltning 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.)

Vid beslut om systemunderhåll ska en projektplan upprättas. Denna ska minst omfatta:

- Tidplan.
- Resurser. (personella och ekonomiska)
- När och hur uppföljning, utvärdering och avrapportering ska ske.
- När och hur medarbetarna ska informeras och utbildas.
- Målformulering.

Målet med underhållet är beroende av målen med verksamheten och sätts vid verksamhetsplaneringen. Målen med systemunderhållet ska sättas av systemägaren i samråd med IT-beredningsgrupp och ev. styrgrupp. Förslag till årliga mål utarbetas av systemägaren i samråd med IT-beredningsgruppen.

- Budget.

  Systemägaren ansvarar för systemets ekonomi inom ramen för ledningens resurstilldelning. Om krav om åtgärder framkommer i systemsäkerhetsplanen som innebär en kostnad för andra systemägare skall dessa bekostas av systemägaren eller i samråd med IT-beredningsgruppen. Driftbudgeten tas fram i samråd med IT-ansvarig. 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 systemägaren ska 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 ska dokumenteras och arkiveras.

Åtgärd som kan inplaneras:

- Utvecklingsåtgärd planeras in på vanligt sätt av systemägare, IT-beredningsgrupp och leverantör.
- Driftåtgärd planeras in på vanligt sätt av systemägare, IT-beredningsgrupp och leverantör.

Därefter inordnas förändringsförslagen i någon av följande klasser:

- Förberedelse.

  Alla åtgärdsförslag med prioriteringsklass *åtgärd som kan inplaneras* förbereder systemadministratören och IT-

beredningsgruppen. Det huvudsakliga arbetsinnehållet i förberedelsearbetet 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 ska 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 ska 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 ska 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 ska leverantören åtgärda felen och återkomma med ny tid för leverans.

Drift
Möjligheten till en säker och ändamålsenlig drift av ett IT-system är beroende av helhetstäckande och aktuell dokumentation. Kommunens regler för systemdrift ska 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 tekniska IT-infrastruktur ska vara dokumenterad i särskild systemsäkerhetsplan.

Avveckling av IT-system
IT-system som inte längre behövs för verksamheten ska avvecklas snarast. Systemägare ska efter samråd med IT-beredningsgruppen besluta om och när ett IT-system ska avvecklas. En plan för avvecklingen ska upprättas. Planen ska särskilt beakta:

- Rättsliga regler såsom Arkivlagen, PUL.
- Vad som ska 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.

Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Följande rutiner och riktlinjer gäller:

- Vid misstanke om intrång eller andra incidenter ska användare agera enligt IT-säkerhetsinstruktion: Användare.
- IT-säkerhetssamordnaren ska sammanställa och rapportera till ledningen.
- Intrång och försök till intrång.
- Brott mot lagstiftning och internt regelverk.
- Incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar.

IT-incidenthantering
IT-chef ska besluta om vilka som ska ha tillträde till kommunens datorrum. För att kunna följa upp detta ska besök vara loggade.

Säkerhetskopiering och lagring
Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av de systemsäkerhetsplaner som respektive systemägare upprättar. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsplan för IT-infrastrukturen.

Externa anslutningar
Systemägaren ska ta ställning till hur autenticering ska ske vid externa anslutningar.

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.

Distansarbete mm
Arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket är inte tillåtet utan ett godkännande har skett från systemägare och IT-ansvarig. Handdatorer, digitala kameror, mobiltelefoner m.m. får inte anslutas till datorer som inte har ett uppdaterat virusprogram. All kringutrustning ska vara godkänd och installerad av IT-enheten.

Användningen av E-post och Internet
I e-postsystemet ska finnas en loggningsfunktion där inkommande och utgående e-post registreras så att alla meddelanden kan spåras. Loggning ska ske av Internettrafiken för att möjliggöra spårning av intrång och missbruk.

Riktlinjer för användningen av Internet och e-post ska framgå av Säkerhetsinstruktion: Användare och ”Regler och riktlinjer för användare”.

Skyddade identiteter
Speciella rutiner skall upprättas och dokumenteras för att säkerställa att inte skyddade identiteter hanteras på ett oaktsammt sätt så att kommunen eller tredje part lider skada

5 IT-säkerhetsutbildning

Information och utbildning inom IT-säkerhetsområdet ska ges alla medarbetare och omfatta

- IT-säkerhetens betydelse för verksamheten
- Innehållet i kommunens IT-policy
- Tillämpliga delar av innehållet i IT-säkerhetsinstruktionerna: Förvaltning, Användare och Drift

Nya medarbetare ska ges grundläggande säkerhetsutbildning före tilldelning av behörighet i nätverket.

Systemägare ansvarar för

- Att 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.
- Att medarbetare har godkänt ”Regler och riktlinjer för användare”.

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

6 Kontinuitetsplanering

Systemägarnas krav på avbrotts- och katastrofplanering skall vara samordnade i organisationens systemsäkerhetsplan för den tekniska infrastrukturen. Se också IT-säkerhetsinstruktion: Drift.

7 Driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett IT-system uppfyller ställda säkerhetskrav.
I samband med att en systemsäkerhetsplan upprättas granskas om IT-systemet uppfyller:

- Basnivå
- De tilläggskrav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav

Systemägaren beslutar om driftgodkännande. Beslutet baseras på en granskning och säkerhetsutvärdering som bygger på jämförelse mellan verksamheternas krav och vidtagna säkerhetsåtgärder.
Driftgodkännandeprocessen relateras till aktuell systemsäkerhetsplan och ska 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.

8 Revidering och uppföljning

Uppföljning är en viktig del i IT-säkerhetsarbetet.
Uppföljningen ska bevaka:

- Att beslutade åtgärder är genomförda
- Årliga mål är uppfyllda
- Att riktlinjer följs
- Att systemsäkerhetsplaner och strategidokument vid behov revideras

HÄLLEFORS KOMMUN

IT-enheten 712 83 Hällefors
Besöksadress Sikforsvägen 15 Hällefors
Telefon 0591-641 00 vx • Fax 0591-109 76
kommun@hellefors.se