Handläggare
Henrik Andersson

Informationssäkerhetspolicy

Antagen av Kommunfullmäktige 2008-05-05, § 36, reviderad 2014-03-03 § 20
registernr 03.16.2

Innehållsförteckning

Övergripande

INLEDNING

BAKGRUND

Informationssäkerhet syftar till förmågan att upprätthålla önskad sekretess, riktighet och tillgänglighet avseende information och informationstillgångar.
Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer ska så långt som möjligt gälla som ramverk för Informationssäkerhetsarbetet.

ANDRA DOKUMENT

Detta dokument kompletterar det av kommunfullmäktige beslutade ”IT-strategi för Emmaboda kommun”. Där framgår mål, mm för kommunens användning av informationsteknik (IT).

OMFATTNING

Informationssäkerhetspolicyn gäller de system och den information som behandlas med hjälp av informationsteknik. Syftet är att IT skall utnyttjas på ett för medborgare och verksamhet säkert sätt. Policyn omfattar alla verksamheter inom kommunens samtliga förvaltningar och helägda bolag, där vi erbjuder ett samarbete inom vårt datanät.

MÅL FÖR ARBETET MED INFORMATIONSSÄKERHET

ALLMÄNT

Informationssäkerhetspolicyn är en del av kommunens IT-verksamhet och redovisar kommunstyrelsens viljeinriktning och stöd för Informationssäkerhetsarbetet och syftar till att klarlägga:

- mål
- organisation, ansvar och roller
- riktlinjer för områden av särskild betydelse

Policyn konkretiseras i Säkerhetsinstruktionerna: Förvaltning, Drift och Användare samt i Systemsäkerhetsanalyser.

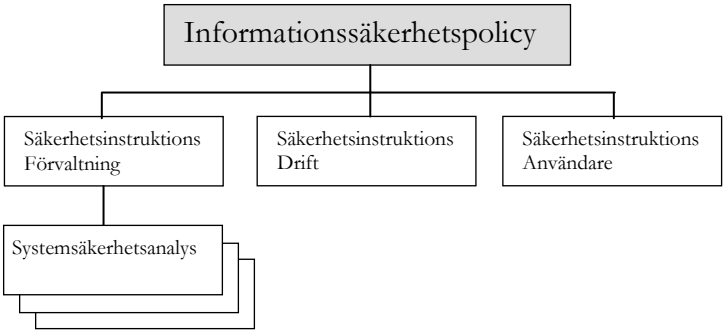

Bild 1 Styrande dokument

Säkerhetsinstruktionerna fastställs av kommunstyrelsen. Systemsäkerhetsanalyserna beslutas av respektive systemägare.

ÖVERGRIPANDE MÅL

Målet för Informationssäkerhetsarbetet är att minimera riskerna för störningar i förvaltningarnas och bolagens verksamheter, på grund av fel i eller felaktig användning av ett eller flera IT-system.

Dessutom ska all användning, administration och utveckling av IT-system ske så:

- att offentlighet, sekretess och medborgarnas rätt till integritet är säkerställd
- att kraven på åtkomst, tillförlitlighet och tillgänglighet uppfylls.

GENERELLA LÅNGSIKTIGA MÅL

För kommunens Informationssäkerhetsarbete ska gälla:

- lagar och föreskrifter följs
- det stöder utvecklingsarbetet
- krishanteringsförmågan säkerställs
- det förebygger oväntade händelser i IT-systemen som kan leda till negativa konsekvenser
- det säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- alla investeringar både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad
- informationen ses som en tillgång och skyddas i paritet med dess värde
- all personal ges kunskap om gällande Informationssäkerhetsregler
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- hotbilden för varje enskilt samhällsviktig IT-system analyseras fortlöpande
- det ska finnas dokumentation av alla IT-system

ORGANISATION, ROLLER OCH ANSVAR

ÖVERGRIPANDE ANSVAR

Det övergripande ansvaret för säkerheten i kommunens IT-verksamhet vilar på kommunstyrelsen.

ROLLER OCH ANSVAR

Organisation, roller och fördelning av ansvar 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 Informationssäkerhetspolicyns mål.

Samtliga IT-system och program ska vara identifierade och förtecknade och kommunchefen utser systemägare för dessa. För de samhällsviktiga IT-systemen ska en systemsäkerhetsanalys upprättas Analysen ska utgöra underlag för systemägares beslut om driftgodkännande. Kommunstyrelsen beslutar vilka IT-system som är samhällsviktiga och för vilka det ska upprättas systemsäkerhetsanalys. De system som är samhällsviktiga är beslutade av Kommunstyrelsen KS/2009:41 §25
Den interna organisationen för Informationssäkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av Informationssäkerhetsinstruktion: Förvaltning.

SÄRSKILDA RUTINER

Vissa delar inom området Informationssäkerhet är av särskild betydelse för kommunens verksamhet. Av Säkerhetsinstruktionerna ska särskilda riktlinjer, regler och rutiner framgå enligt följande:

- **Säkerhetsinstruktion Förvaltning:** Behörighetsadministration, behörighetskontroll, loggning och spårbarhet, distansarbete, drift- och förvaltning, tillträdesskydd, säkerhetskopiering och lagring, avveckling av datamedia och datakommunikation.

- **Säkerhetsinstruktion Användare:** Informationshantering, distansarbete, IT-incidenthantering, säkerhetskopiering och lagring, e-post och användning av Internet.

- **Säkerhetsinstruktion Drift:** System- och driftdokumentationer, förvaring av datamedia, bemanning, tillträdes- och brandskydd, elförsörjning, regler för säkerhetskopiering och förvaring av datamedia. (Säkerhetsinstruktion Drift ska utarbetas av IT-chefen snarast efter det att Systemägarnas krav framförts i Systemsäkerhetsanalyserna.)

REVIDERING OCH UPPFÖLJNING

Uppföljning är en viktig del av Informationssäkerhetsarbetet.

Uppföljningen ska bevaka

- att beslutade åtgärder är genomförda
- att mål är uppfyllda
- att riktlinjer följs

Policy, Säkerhetsinstruktioner och Systemsäkerhetsanalyser ska löpande följas upp årligen och vid behov revideras

Säkerhetsinstruktion Förvaltning

INLEDNING

Säkerhetsinstruktion Förvaltnings roll i informationssäkerhetsarbetet:

Informationssäkerhet syftar till förmågan att upprätthålla önskad sekretess, riktighet och tillgänglighet avseende information och informationstillgångar.

Styrande dokument för *IT-säkerhetsarbetet* är Informationssäkerhetspolicyn samt Säkerhetsinstruktionerna: Förvaltning, Drift och Användare. Säkerhetsinstruktionerna är en konkretisering av Informationssäkerhetspolicyn.
Krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en *systemsäkerhetsanalys*. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten.

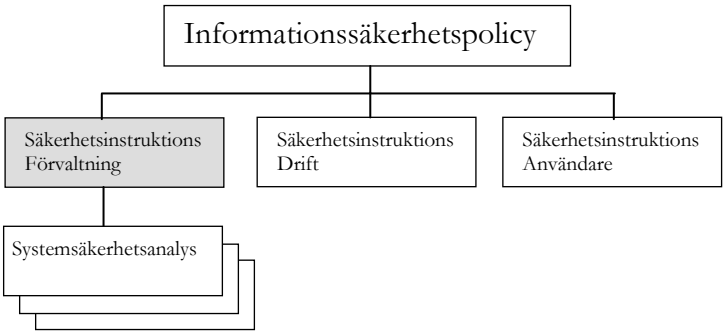

Bild 1 Styrande dokument

Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för IT-säkerhetsarbetet. Detta dokument, Säkerhetsinstruktion Förvaltning, utgår från Informationssäkerhetspolicyn och syftar till att redovisa:

- organisation för IT-säkerhetsarbetet
- beskriva roller och ansvar för IT-säkerhetsarbetet
- beskriva hur IT-säkerhetsarbetet ska bedrivas
- ange särskilda rutiner som kan vara aktuella

ORGANISATION OCH ANSVAR

Kommunfullmäktige fastställer Informationssäkerhetspolicyn och Säkerhetsinstruktioner för Förvaltning, Drift och Användare.

Ansvaret för informationssäkerheten följer linjeorganisationen för varje enskilt IT-system. Förvaltningschef/vd är i regel systemägare och ansvarig för IT-system som stödjer den egna verksamheten. IT-chefen är systemägare för kommunens tekniska infrastruktur-IT.

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 Informationssäkerhetspolicyns mål.

För varje IT-system utses nedanstående roller för att ge en tydlig ansvarsfördelning. I vissa fall kan samma person inneha flera av dessa roller.
IT-säkerhetsfunktionen och IT-säkerhetssamordnare gäller generellt för hela kommunkoncernen.

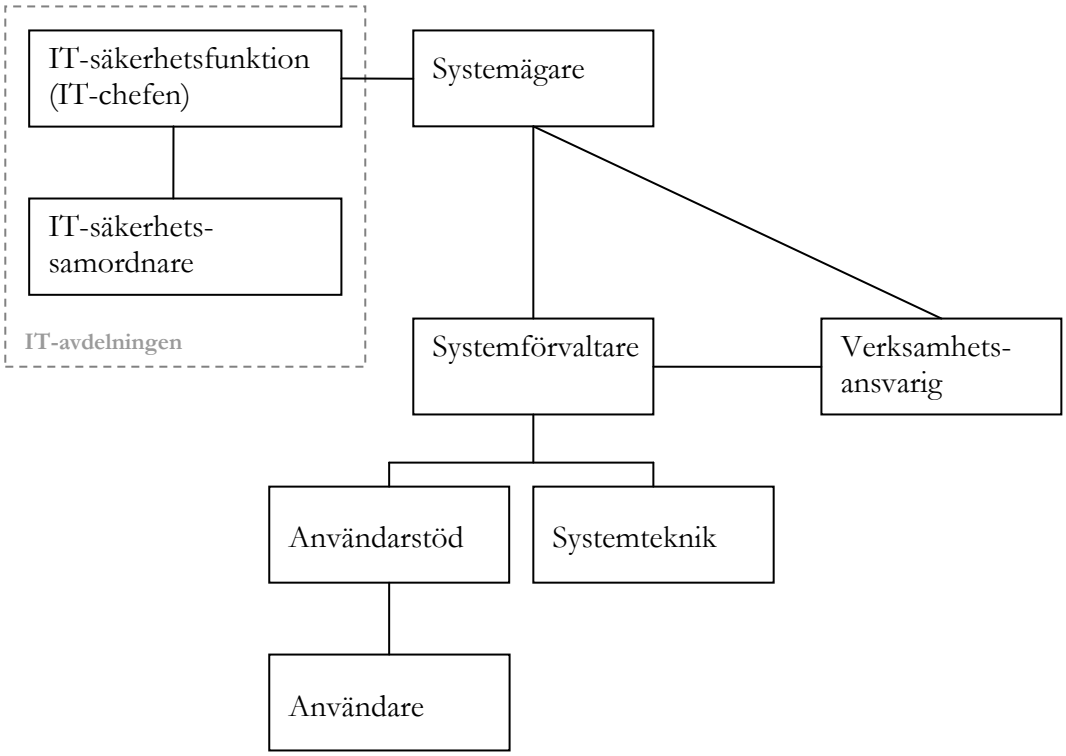

Bild 2 Roller inom IT-säkerhetsområdet

ÖVERGRIPANDE ANSVAR

Det övergripande ansvaret för kommunens IT-system vilar på kommunstyrelsen. Kommunstyrelsen beslutar om vilka IT-system som är samhällsviktiga. Systemägare för dessa samhällsviktiga system ansvarar för att en systemsäkerhetsanalys avseende risk och sårbarhet upprättas. De system som är samhällsviktiga är beslutade av Kommunstyrelsen KS/2009:41 §25

SYSTEMÄGARE

Systemägaren ansvarar inför kommunstyrelsen för att egna IT-system förvaltas på för verksamheten bästa sätt. Vid nyutveckling eller större förändringar av datasystem ska systemägaren alltid samråda med IT-chefen 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 tilldelade resurser:

- att fatta de avgörande besluten om IT-systemets nyinvesteringar, vidareutveckling och avveckling
- att fastställa säkerhetsnivån för det enskilda IT-systemet.
- att IT-systemets funktioner och tekniska lösning följer gällande lagstiftning
- tillsätta organisation och befattningar som rör systemet t.ex. systemförvaltare och användarstöd
- att systemet är väldokumenterat
- att systemet finns registrerat i en förteckning innehållande en sammanfattande beskrivning av nämndens respektive bolagets samtliga IT-system
- att säkerhetsanalys av IT-systemet utförs
- att delta i och stödja IT-säkerhetsarbetet
- att om så beslutats upprätta en systemsäkerhetsanalys
- att i systemsäkerhetsanalysen 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 ska gälla
  - omfattning av loggning
  - hur loggar ska 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

- att fastställa IT-systemets dokumentation och användarhandledning
- utbildning som rör systemet
- att fatta beslut om förvaltning av IT-systemet
- att lämna förslag på att system som inte i tillräcklig grad är till gagn för verksamheten avvecklas
- att behövliga licenser respektive tillstånd finns
- att i samverkan med IT-chef fastställa avbrottsplan för IT-systemet
- att driftgodkänna IT-systemet

SYSTEMFÖRVALTARE

Systemförvaltare utses av systemägaren och är den person i berörd verksamhet som har ansvaret för den dagliga användningen och förvaltningen av IT-systemet. I detta ingår

- att delta i och stödja IT-säkerhetsarbetet
- att verkställa systemägarens beslut
- att sköta användar- och behörighetsadministration
- att behörighetstilldelningen till IT-systemet sker på avsett sätt
- att hålla sig informerad om utvecklingen av systemet och påtala behov av förändringar till systemägaren
- att dokumentera uppkomna fel, brister och incidenter i systemet och rapportera dessa till systemägaren och IT-säkerhetssamordnaren
- 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 användarsstöd beträffande verksamhetsrelaterade frågor i systemet
- att samverka med IT-avdelningen och delta i arbetet med säkerhetsfrågor som rör systemet
- att vara kontaktperson mot IT-avdelningen
- att i samverkan med IT-avdelningen ta fram installationsanvisning för systemet
- att reservrutiner enligt kontinuitetsplaneringen är kända
- att driften och utvecklingen av IT-systemet följer fastställd säkerhetsnivå

- att användarna av IT-systemet får erforderlig utbildning och information om specifika användarinstruktioner för systemet.
- att samverka med funktionerna för användarstöd och systemteknik, för att säkerställa driften av IT-systemet

ANVÄNDARSTÖD

Användarstödfunktionen, som utgörs av en eller flera personer, utses av systemägaren.

Användarstödfunktionen bistår systemförvaltare med stöd till användarna av systemet.

SYSTEMTEKNIK

Funktionen för systemteknik utgörs av kommunens IT-avdelning, om inte annat anges i systemsäkerhetsanalysen för respektive system.

Systemteknikfunktionen utför på uppdrag av systemägaren eller systemförvaltare överenskomna tekniska drift- och servicerutiner.

Systemteknikfunktionen har tillgång till installationsanvisningar från respektive systemförvaltare.

Systemteknikfunktionen innehar den tekniska kompetensen och ansvarar tillsammans med systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-chefen.

Systemteknikfunktionen har bl a följande uppgifter:

- registrera/avregistrera användare i systemet (infrastrukturen) med den behörighetsprofil som systemägaren har beslutat
- tillhandahålla teknisk support
- delta i och stödja IT-säkerhetsarbetet
- initiera felsökning vid driftsstörningar och vidta nödvändiga åtgärder och dokumentera dessa
- ansvara för att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs

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 Säkerhetsinstruktion Användare
- rapportera olika former av fel, brister och incidenter enligt fastställda rutiner
- föreslå förändringar till verksamhetsansvarig
- påtala behov av utbildning

VERKSAMHETSANSVARIG

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 används 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 ska registreras (registeransvarig)
- tillse att systemet följer Personuppgiftslagen, PUL
- att ansvara för vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen och hur detta ska ske
- att besluta om och beställa (skriftligt) enskilda användares behörighet till IT-systemet
- att besluta hur och av vem informationen ska registreras i systemet
- att anmäla till systemförvaltare när personal slutar eller av annat skäl ska ha ändrade behörigheter

IT-SÄKERHETSFUNKTION

IT-chefen är ansvarig för IT-säkerhetsfunktionen. IT-chefen är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar. IT-chefen samverkar med systemägare vad avser drift och resurstilldelning för ett IT-system.

IT-chefen har bl a ansvar för:

- att systemsäkerhetsanalys för teknisk IT-infrastruktur upprättas och hålls aktuell
- att delta i och stödja IT-säkerhetsarbetet
- att efter beställning tilldela och administrera behörigheter till den gemensamma infrastrukturen
- utformning av förslag på den strategiskt långsiktiga och övergripande IT-utvecklingen
- att omvärldsbevakning sker
- att i samråd med systemägare se till att systemet fungerar ihop med samverkande IT-system
- att testmiljö finns tillgänglig vid behov
- att teknisk IT-infrastruktur hålls uppdaterad med buggfixar och säkerhetsuppdateringar
- att rutiner för säkerhetskopiering uppfyller systemägarnas krav
- 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
- att biträda systemägarna i avbrottsplaneringen
- att vara teknisk rådgivare till systemägarna då förändringar i systemen är aktuella
- att den tekniska IT-infrastrukturens säkerhet motsvarar systemägarnas krav och uppfyller krav enligt systemsäkerhetsanalyserna
- att ett IT-system håller den tekniska och funktionella kvalitet som överenskommits med systemägaren.
- administration av organisationens brandväggar och skydd mot skadlig kod
- att Säkerhetsinstruktion Drift är aktuell
- att stödja systemägarna i IT-säkerhetsarbetet

IT-UTVECKLINGSGRUPP

IT-Utvecklingsgrupp stödjer det tekniska arbetet med att uppnå Informationssäkerhetspolicyns mål. Detta kan innebära aktivt deltagande i projekt, utvärdering och diskussioner kring metoder, plattformar eller IT-system. IT-Utvecklingsgrupp kan sägas arbeta som teknisk konsult åt verksamheten och är direkt underställd IT-chefen. IT-Utvecklingsgrupp har till uppgift att i ett tekniskt perspektiv:

- följa upp att Informationssäkerhetspolicyn och Säkerhetsinstruktionerna revideras och hålls aktuella
- vara rådgivande i IT-säkerhetsfrågor
- stödja IT-chefen vid upprättande av kontinuitetsplan för teknisk IT-infrastruktur
- stödja systemägarna vid:
  - upprättande av systemsäkerhetsanalys
  - upprättande av systemspecifika säkerhetsinstruktioner
  - upprättande av kontinuitetsplanering för verksamheten
  - säkerhetsgranskning inför driftgodkännande
  - utbildning i IT-säkerhetsfrågor
- sammanställa och rapportera IT-säkerhetsincidenter
- följa upp hur Informationssäkerhetspolicyn efterlevs

INSTRUKTION FÖR IT-SÄKERHET

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

- Innehållet i Informationssäkerhetspolicyn
- Tillämpliga delar av innehållet i Säkerhetsinstruktionerna Förvaltning, Användare och Drift

Nya medarbetare ska ges information om säkerhetsfrågor före tilldelning av behörighet i nätverket. Närmaste chef ansvarar för att informera om Informationssäkerhetspolicyn och Säkerhetsinstruktion Användare.

Systemägare ansvarar för

- att egna medarbetare erhåller information och utbildning om innehållet i de systemsäkerhetsanalyser de är berörda av
- att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om säkerhetsreglerna för de IT-system de ska ha tillgång till.

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

SÄRSKILDA RUTINER

ÅTKOMST TILL IT-RESURSER

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

BEHÖRIGHETSADMINISTRATION

Beställning av åtkomst till IT-infrastrukturen (Filserver, e-post, mm) ska ske hos IT-avdelningen, IT-samordnare eller verksamhetsansvarig. Chefen är behörig beställare.

Om medarbetare ska ha behörighet till ett verksamhetssystem ska verksamhetsansvarig chef beställa behörighet hos respektive systemförvaltare.

BEHÖRIGHETSKONTROLL

Leverantörslösenord och behörigheter ska förvaras säkert. Leverantörslösenord är ofta standardiserade och ska därför ändras.

LOGGNING OCH SPÅRBARHET

Systemägarnas krav på säkerhets- och transaktionsloggar ska framgå av de systemsäkerhetsanalyser som respektive systemägare upprättar.

DISTANSARBETE, EXTERN ANSLUTNING OCH MOBIL DATORANVÄNDNING

Verksamhetsansvarig chef (Förv. chef/VD) beslutar om ett IT-systems information ska få hanteras utanför arbetsplatsen med stationär eller mobil utrustning. Organiserat distansarbete ska arbetsrättsligt vara reglerat i kollektivavtal mellan arbetsgivaren och den anställde.

För extern anslutning och mobil datoranvändning ska särskilda riktlinjer finnas. (Se Säkerhetsinstruktion Användare).

Verksamhetens riktlinjer 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)
- hantering av information på mobila enheter som USB-minne, bärbar dator, telefoner mm.
- om lagring och säkerhetskopiering av information ska ske i egen dator eller hos arbetsgivaren (stöldrisk, obehörig tillgång och förstörelse m.m.)

DRIFT- OCH FÖRVALTNING AV IT-SYSTEM

INFÖRANDE AV IT-SYSTEM

Innan införande av IT-system bör en risk- och sårbarhetsanalys göras. Den utgör ett viktigt underlag för den kravspecifikation som ska upprättas och syftar bl. a. till att klarlägga de säkerhetskrav som verksamheten 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
- tidplan
- resurser (personella och ekonomiska)
- när och hur uppföljning, utvärdering och avrapportering ska ske
- när och hur medarbetarna ska informeras och utbildas

AVVECKLING AV IT-SYSTEM

IT-system som inte längre behövs för verksamheten ska avvecklas snarast. Systemägare beslutar om och när ett IT-system ska avvecklas. Vid avveckling ska särskilt uppmärksammas:

- Rättsliga regler såsom Arkivlagen, PUL
- Vad ska tas ut ur systemet före avveckling (på papper eller media)
- Innehåller systemet ärenden vilka behöver avslutas i diariet
- Behöver återläsning av innehåll kunna ske längre fram
- Behöver uppgifter flyttas över till annat IT-system
- Destruktion av media som innehållit information
- Regler för destruktion av media som innehållit sekretessbelagd information

DRIFT

Kommunens regler för systemdrift ska vara samlade i Säkerhetsinstruktion Drift som ska innehålla:

- Systemdokumentationer
- Driftdokumentationer
- Bemanningsplan (nyckelpersonberoende)
- Tillträdes- och brandskydd
- Elförsörjning
- Regler för säkerhetskopiering
- Regler för förvaring av datamedia
- Regler för avveckling av datamedia

Den tekniska IT-infrastrukturen ska vara dokumenterad i särskild systemsäkerhetsanalys.

IT-INCIDENTHANTERING

Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Riktlinjer för hur incidenter följs upp är därför angelägna. Följande gäller:

- vid misstanke om intrång eller andra incidenter ska användare agera enligt Säkerhetsinstruktion Användare

Systemförvaltaren ska sammanställa och rapportera till IT-chefen.

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

IT-chefen rapporterar till IT-Utvecklingsgrupp.

TILLTRÄDESSKYDD

IT-chefen ska besluta om vilka som ska ha tillträde till serverrum.

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 systemsäkerhetsanalys för IT-infrastrukturen.

AVVECKLING AV DATAMEDIA

Datamedia med sekretessbelagd information ska avvecklas i enlighet med systemägarens instruktioner.

DATAKOMMUNIKATION

INTERN KOMMUNIKATION

Kommunens nät ska vara väl dokumenterat.

EXTERNA ANSLUTNINGAR

Kommunen är för sin verksamhet beroende av datakommunikation med medborgarna, andra organisationer och centrala myndigheter främst via Internet.

Följande riktlinjer gäller:

- IT-chefen upprättar och godkänner anslutning till kommunens nät.
- För att försvåra för obehöriga att göra intrång i organisationens datasystem via externa anslutningar ska det finnas en s k brandvägg installerad
- Kontroller ska ske av vem som får släppas in
- En kontrollista på vilka nätverksadresser och IP-portar som är tillåtna ska användas för att filtrera bort onödig trafik
- Användningen av tjänster ska fastställas och dokumenteras vad gäller kommunikationsriktning, vilka protokoll som ska stödjas samt vilka applikationer som använder protokollen

BRANDVÄGGAR

IT-chefen 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

ANVÄNDNINGEN AV E-POST OCH INTERNET

Riktlinjer för användningen av Internet och e-post ska framgå av Säkerhetsinstruktion Användare.

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.

KONTINUITETSPLANERING

Av systemsäkerhetsanalyserna ska framgå de enskilda IT-systemens krav på avbrotts- och katastrofplanering. Kraven ska vara sammanställda i systemsäkerhetsanalysen för den tekniska infrastrukturen.

DRIFTGODKÄNNANDE

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

I samband med att en systemsäkerhetsanalys 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 systemsäkerhetsanalys och ska omfatta;

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

Beslutsunderlaget ska innehålla en sammanfattning av förslag till beslut som kan vara att;

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

Säkerhetsinstruktion Användare

UPPSLAGSVERK

Se gärna detta dokument som ett uppslagsverk och en viktig källa om hur IT-systemen och informationen får användas. Saknar du någon information eller vill du veta mera så tveka inte att kontakta IT-avdelningen eller närmaste chef.

ALLMÄNT

Användningen av IT-stöd i vårt dagliga arbete ökar och införandet av fler strategiska IT-tillämpningar sker kontinuerligt. För att alla dessa system ska vara säkra, tillgängliga och fungera som det effektiva verktyg vi önskar, är det viktigt att användningen sker på ett kontrollerat sätt. En förutsättning för detta är att du känner till de krav som ställs på dig som IT-användare.

Du måste veta:

- vilket ansvar du har
- vad du ska göra vid olika situationer och incidenter
- hur du ska hantera de verksamhetsbaserade informationssystemen
- hur du får använda e-post och Internet

STYRANDE DOKUMENT

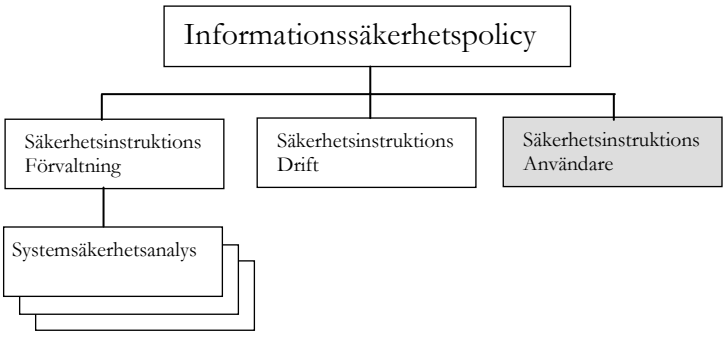

Bild 1 Styrande dokument

Informationssäkerhet ska upprätthålla önskad sekretess, riktighet och tillgänglighet avseende information och informationstillgångar.

Informationssäkerhetspolicyn redovisar kommunstyrelsens viljeinriktning och mål för IT-säkerhetsarbetet och syftar till att klarlägga:

- organisation och roller för IT-säkerhetsarbetet
- krav på riktlinjer för områden av särskild betydelse

Policyn konkretiseras i tre säkerhetsinstruktioner:

Säkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna
- de riktlinjer som gäller för områden av särskild betydelse

Säkerhetsinstruktion Drift redovisar:

- organisation och ansvar för drift av IT-systemen
- regler och rutiner för vissa områden
- regler för systemutveckling, systemunderhåll, incidenthantering
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Säkerhetsinstruktion Användare, som syftar till att ge dig som användare kunskaper och riktlinjer om hur du arbetar för att Emmaboda kommun ska hålla en hög och bra IT-säkerhet.

Kommunstyrelsen beslutar om vilka IT-system som är samhällsviktiga. Varje sådant IT-system ska dokumenteras i en systemsäkerhetsanalys. De system som är samhällsviktiga är beslutade av Kommunstyrelsen KS/2009:41 §25

ORGANISATION OCH ROLLFÖRDELNING

Det övergripande ansvaret för kommunens IT-system vilar på kommunstyrelsen. Kommunchefen utser systemägare för vart och ett av kommunens IT-system. En IT-styrgrupp inrättas för samordning och behandling av övergripande gemensamma IT-frågor.

Systemägare - Systemägaren (i regel förvaltningschef/vd) initierar den egna verksamhetens behov av IT-stöd. Systemägaren har det övergripande ansvaret inför kommunstyrelsen att ett IT-system förvaltas på för verksamheten bästa sätt. Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-system inom ramen för resurstilldelningen för sin verksamhet.

Verksamhetsansvarig – ansvarig för informationen och utsedd av systemägaren. Beslutar om behörigheter, är registeransvarig, ser till att informationen följer Personuppgiftslagen, avgör vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen, mm.

Systemförvaltare - Operativt ansvarig och utsedd av systemägaren, är den person som har ansvaret för den dagliga användningen av IT-systemet. Systemförvaltare samverkar med IT-avdelningen för att säkerställa en säker och rationell drift av systemet.

IT-chef - är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar. IT-chefen samverkar med systemägare vad avser drift och resurstilldelning för ett IT-system. IT-chefen understödjer arbetet med att uppnå målen i Informationssäkerhetspolicyn och är ansvarig för att samordna IT-säkerhetsarbetet inom kommunen.

Ansvarig IT-tekniker - tillhör IT-avdelningen och utses av IT-chefen. Innehar den tekniska kompetensen och ansvarar tillsammans med systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-chefen.

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 Säkerhetsinstruktion Användare
- rapportera olika former fel, brister och incidenter, t ex misstänkt virusangrepp enligt fastställda rutiner
- föreslå förändringar till verksamhetsansvarig
- påtala egna behov av utbildning

INLOGGNING OCH LÖSENORD

BEHÖRIGHET

Våra IT-system är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef.

För att få behörighet krävs att

- du av din chef fått information om innehållet i denna säkerhetsinstruktion och om kommunens Informationssäkerhetspolicy,
- att du fått utbildning på de system du kommer att använda.

LÖSENORD

Lösenordet är strängt personligt och ska hanteras därefter. Tänk på att du själv kan bli misstänkt om någon använder ditt lösenord för olämpliga ändamål. Du ska därför:

- inte avslöja ditt lösenord för andra eller låna ut din behörighet
- skydda lösenordet väl
- omedelbart byta lösenord om du misstänker att någon känner till det
- byta lösenordet enligt de regler som gäller för respektive system.

För att väsentligt försvåra lösenordsknäckning bör bokstäver, siffror och specialtecken blandas i lösenordet.
Viktigast av allt är dock att du väljer ett lösenord som du kommer ihåg.

Om du glömmer ditt lösenord och försöker logga in till systemet med ett felaktigt sådant, kan din användaridentitet låsas. Antalet inloggningsförsök och annat som berör inloggning bestäms av systemägaren. Om detta inträffar vänder du dig till systemförvaltaren eller IT-avdelningen.

BESÖKARE – INLOGGNING OCH DATOR

För besökande, konsulter mfl som behöver tillgång till dator på vårt nät kan IT-avdelningen öppna ett tillfälligt användarkonto som sedan spärras automatiskt.
Besökande får inte koppla in sin medhavda dator på vårt nät. (Undantag de sammanträdesrum som har särskilt nätuttag för besökande, med enbart åtkomst till Internet.) Koppling till projektor möter inget hinder. Besökande kan under uppsikt använda våra datorer och t ex ha med sin presentation på extern media.
Undantag från ovanstående kan ske efter samråd med IT-avdelningen.

HANTERING AV INFORMATION

ALLMÄNT

I ditt dagliga arbete kommer du i kontakt med information i många olika former. Informationen kan vara talad, på papper, lagrad i datorer via e-post m.m. För att du ska få den information som du behöver, vid rätt tidpunkt och med korrekt innehåll har vi som övergripande mål för informationssäkerhetsarbetet att vi ska:

- behandla information på ett tydligt, korrekt, säkert och relevant sätt
- kunna leverera och hämta information vid rätt tidpunkt
- uppnå och upprätthålla en god informationssäkerhet

Med dessa mål som bakgrund utgår kommunen från synsättet att våra medarbetare ska ha tillgång endast till den information och de system de behöver för sitt arbete.

En stor mängd handlingar (uppgifter) kan vara sekretesskyddade. Det är viktigt att du är förtrogen med karaktären på de handlingar/uppgifter som du hanterar.

ALLMÄN HANDLING

Handlingar kan vara allmänna eller icke allmänna. Allmänna handlingar kan sedan vara offentliga eller hemliga . Vissa allmänna handlingar måste registreras, arkiveras och diarieföras. Det gäller även handlingar som inkommer via telefax, e-post mm.

Huvudregeln är att allmänna handlingar är tillgängliga för den som vill ta del av dem. Om du är tveksam ska du kontakta kansliavdelningen. En begäran om allmän handling ska åtgärdas skyndsamt. Det innebär dock att du alltid kan ta den tid du behöver för att fråga om råd.

PERSONUPPGIFT

I personuppgiftslagen, PUL, regleras rätten att behandla personuppgifter. Syftet med personuppgiftslagen är skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Om du behöver upprätta särskilda register för uppföljning, kvalitetskontroll och forskning bör du samråda med Kansliavdelningens personuppgiftsombud eller personuppgiftsansvarige i ett tidigt stadium i planeringen av registret.

LAGRING AV INFORMATION

Det finns två olika typer av lagringsmöjligheter.

- **Information i våra verksamhetssystem**

Som stöd i det dagliga arbetet har vi flera olika IT-baserade verksamhetssystem som ekonomi- och lönesystem, system för elevadministration och journalhantering, m fl. I dessa system finns inbyggda regelverk som ger rättigheter eller sätter begränsningar för dig att hantera informationen.

För vart och ett av verksamhetssystemen ska det finnas en handbok eller en användarinstruktion, som beskriver vilken information systemet innehåller, vad du ska och får tillföra, ändra och eventuellt ta bort. Det ska också finnas regler för om informationen får kopieras till flyttbara media eller bärbara datorer och om den får hanteras utanför kommunens lokaler.

- **Egna register/dokument**
Utöver att arbeta i våra verksamhetssystem kommer du kanske att upprätta egna register, handlingar och dokument, exempelvis med Word eller Excel. Verksamhetssystemens ”inbyggda skydd” används inte då. Detta kräver särskild uppmärksamhet.

Oavsett om du använder verksamhetssystem eller har skapat egna dokument så har du ett personligt ansvar för säkerheten i din hantering av information:
Du själv måste känna till de regler som gäller.
Du är ansvarig för informationens riktighet och att informationen skyddas mot obehörig insyn.
Samråd med din närmaste chef om du känner dig osäker.

Den information du lagrar på våra gemensamma utrymmen, som kan nås via nätet, säkerhetskopieras enligt de anvisningar regler som system.

G: (Gemensam enhet) är en enhet för lagring av information som du och medarbetarna på din enhet har tillgång till. Här ska merparten av all information lagras. Den blir därmed åtkomlig för andra som har rätt behörighet.

H: (Personlig hemkatalog) är din personliga enhet som du kan använda för lagring av personligt arbetsmaterial. Om du väljer H-enheten kommer dina medarbetare inte åt informationen. Färdigt material ska flyttas över till lämplig mapp på G:

På din lokala hårddisk (C:) ska inget arbetsmaterial lagras eftersom du är personligen ansvarig för att säkerhetskopiering sker. Om du lagrar information på din lokala hårddisk (C:) riskerar du att förlora information som inte kan återskapas till rimliga kostnader (arbetstid).

Verksamhetssystem: Är ett system som verksamheten har valt för hantering av handlingar i registrering och diarieföring

IT-SÄKERHET OCH KRINGUTRUSTNING

ALLMÄNT

För att uppnå nödvändig IT-säkerhet finns regler och rekommendationer för användning av våra IT-system:

- Program som ska användas i verksamheten ska gå genom IT-avdelningen.
- All installation och konfiguration av datorer mm ska ske av IT-avdelningen så att kommunens standard följs.
- Enbart enheter som godkänts av IT-avdelningen får anslutas till vårt nät.
- Inköp av datorer, skrivare, mm ska göras via kommunens gällande leveransavtal och IT-avdelningen svarar för alla inköp.
- Det är inte tillåtet att kopiera kommunens program för användning på andra datorer.

- Vid tillfällen när du inte har uppsikt över din dator ska du låsa den. Vid arbetsdagens slut ska du logga ut och stänga av datorn.
- Din enhet med tillhörande hårdvara är kommunens egendom och får inte bytas, förändras eller medtagas utan IT-avdelningens och verksamhetschefens medgivande.
- Inför service på din utrustning som innebär att din enhet lämnas bort eller kasseras måste känslig information tas bort. Detta är särskilt viktigt när det gäller portabla enheter.

MOBILA ENHETER

Arbete utanför kommunens lokaler som kräver uppkoppling mot det interna nätverket får ske enbart via lösning som tillhandahålls av IT-avdelningen. Om du har en privat dator eller annan enhet som du använder för arbete hemma kan denna utgöra en säkerhetsrisk. Du ansvarar för att säkerheten blir bästa möjliga. Tänk på:

- att kontrollera med din chef om det är tillåtet att kopiera informationen till flyttbart media som du sedan t ex tar med hem. Risk finns att obehöriga då kan ta del av den.
- att du inte får lagra sekretessbelagd eller för verksamheten känslig information på privat enhet..
- att om information kopieras mellan arbetsdator och annan dator med t ex extern media är du ansvarig för att den andra datorn har samma säkerhet som din egna.
- Det är din chef som bestämmer om du ska ha möjlighet att arbeta hemifrån eller inte.

KRINGUTRUSTNING MED MELLANLAGRINGSMÖJLIGHET

Handdatorer, digitala kameror, mobiltelefoner mm kan lätt bli virusbärare då du kan mellanlagra information i dessa. Därför ska du inte ansluta denna typ av kringutrustning mot en dator som du inte med säkerhet vet har ett uppdaterat virusprogram.

VÅRT LOKALA NÄTVERK (LAN)

Nätverket är en mycket viktig gemensam resurs som ger oss alla möjlighet att lagra och nå information, dela på skrivare och program, upprätta kommunikation mm.

Följande regler gäller för nätverket:

- Utskrifter av dokument på gemensam skrivare ska snarast hämtas.
- Inloggning på nätverket ska ske med ditt personliga lösenord. (Undantag finns för vissa funktioner.)
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden.
- När du arbetar i kommunens nätverk loggas och registreras i allmänhet dina aktiviteter. Loggningsfunktioner används för att spåra obehörig verksamhet och intrång. Detta görs för att skydda informationen samt för att undvika att oskyldiga misstänks om oegentligheter inträffar.
- Information som sparas på gemensamma utrymmen i det lokala nätverket, ska lagras på anvisad plats.

- Det är förbjudet att ansluta någon utrustning (förutom vanlig fax och telefon) till telenätet.
- Det är förbjudet att skaffa sig utökade systemrättigheter än de som tilldelats.
- Det är absolut förbjudet att försöka göra utrustning eller information på kommunens nät, åtkomlig utifrån.

Om vi alla följer dessa regler så försvårar vi för obehöriga att komma åt informationen. Kom ihåg att du ansvarar för allt som registrerats med din användaridentitet.

INTERNET OCH E-POST

Tänk på att du aldrig kan vara anonym på Internet. Din användning lämnar spår i din egen dator, i kommunens loggfiler, i operatörernas loggfiler och på de platser du besöker på nätet.

LOGGAR

All användning av Internet registreras i en logg. Loggningen omfattar bl.a. uppgifter om dator och vilken webbplats som besökts. Det förs även en logg över all e-post som innefattar uppgifter om avsändare, mottagare, ärendemening, tidpunkt och storlek på meddelandet samt namnet på bifogade filer.

Granskning av loggar beslutas av IT-chefen som också är PUL-ansvarig för dessa. Syftet med loggarna är främst för teknisk analys men också för att kunna kontrollera att denna Säkerhetsinstruktion efterlevs. Resultatet lämnas ut till den som begärt granskning (se ”Felaktig användning av IT, sid 13). Övrig granskning sker vid tekniska trafikmässiga störningar och problem i Internet-trafiken eller vid så kallad abuse. Abuse är klagomål från andra resursägare ute på Internet och kan gälla att användare brutit mot den rådande nätetiketten. Granskning sker också efter begäran från polisen.
Loggarna är allmän handling och sparas i sex månader.

INTERNET

Tillgången till Internet är ett arbetsverktyg. När du använder Internet kan säkerheten i vårt lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. När du arbetar med program som har direktkontakt med Internet, t ex e-post, webbläsare, meddelandeprogram (Chat), mm, ska du vara extra försiktig och inte ta emot eller öppna filer som du inte helt säkert vet är ofarliga.

Kommunen förutsätter att den som laddar ner filer från Internet har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välrenommerade webbplatser. Distribution eller kopiering av material som är skyddat med upphovsrätt, t ex musik, film och program är förbjudet. Utöver säkerhetsrisken kan detta leda till skadeståndskrav t ex vid brott mot upphovsrätten.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, etc) eller har anknytning till kriminell verksamhet. I specifika fall kan det dock vara motiverat för arbetet, t ex vid utredningar, omvärldsanalyser mm, att besöka sidor som normalt är förbjudna.

När du surfar på Internet representerar du Emmaboda kommun. Gör det med ett gott omdöme så att ditt agerande på nätet inte skadar oss och agera i enlighet med våra värderingar. Tänk på att loggfiler är offentlig handling som visar din aktivitet på Internet samt vilka webbplatser du har besökt.

Även cookies och historikfiler som sparas på din dator innehåller information om vart du surfat. Dessa filer är också allmän handling.

E-POST

E-post omfattas av samma offentlighetsregler som andra typer av handlingar. E-post som ska bevaras och registreras skriver du ut på papper och arkiverar på samma sätt som andra liknande dokument. Föreskrifter om dokumenthanteringen finns i arkiveringsplanen, som är upprättad för din verksamhet.

E-post är ett rationellt hjälpmedel i arbetet men lagringskapaciteten för det är begränsad. Tänk därför på att regelbundet gallra i mapparna för att frigöra utrymme så att inte din e-post spärras. E-postsystemet ska inte användas som ett arkivsystem, bifogade filer mm som du vill spara, sparar du på samma sätt som du lagrar annan information.

Förvaltningslagen reglerar vår skyldighet att ta emot e-post från medborgarna samt vår serviceskyldighet att svara skyndsamt. Din e-post får därmed inte lämnas oläst och obesvarad under semester, sjukdom eller annan ledighet. Vid längre ledighet bör du vidarebefordra din e-post till kollega som är insatt i dina uppgifter. Om du under en kortare tid inte har möjlighet att läsa din e-post ska du aktivera frånvarohanteraren med meddelande om när du återkommer och eventuellt hänvisa till annan tjänsteman.

ALLMÄNT

- e-postsystemet är ett arbetsverktyg.
- det är samma regler för diarieföring av e-post, som för vanliga brev.
- om du misstänker att det kommit in virus via e-postsystemet ska du agera som beskrivits i avsnittet om Incidenter, se nedan.
- e-post som skrivs eller tas emot på arbetsgivarens system tillhör alltid arbetsgivaren enligt prejudicerande fall. Arbetsgivaren får normalt inte läsa anställdas e-post utan att informera om detta i förväg.
- arbetsgivaren kan komma att granska även privat e-post om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet.
- arbetsgivaren kan även granska privat e-post om det är fara för informationssäkerhet t ex virus- eller hackerangrepp, eller för att utreda och förhindra brott.
- chef kan begära hos IT-chefen att ge anställd rätt att läsa e-post ställd till en kollega som har semester, är tjänstledig eller är sjuk. Chef ska om möjligt inhämta medgivande från e-postmottagaren.
- e-postlista, dvs förteckning över inkommen och skickad e-post (avsändare och ärendemening) är allmän handling och ska behandlas enligt offentlighetsprincipen.

ANVÄNDNING

- du ska följa de råd om inställningar i och hantering av e-postsystemet som du får av IT-avdelningen.
- Vidaresändning av e-post externt ska behandlas med försiktighet.
- ange alltid ämne för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-brevet.
- kontrollera vilka som är medlemmar på sändlistor innan du använder dem.

- du bör vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer.
- skicka inte och vidarebefordra inte kedjebrev av någon sort.
- fundera på vart du lämnar ut din e-postadress, på mindre seriösa ställen kan det resultera i skräppost (spam).
- notera också att användning av gratisprogram ofta resulterar i att programmet dolt för dig, skickar din e-postadress vilket kan resultera i skräppost
- stryk dig från e-postlistor om du inte vill ha fler brev via dem eller är frånvarande en längre tid
- använd inte heller din vanliga användaridentitet och ditt lösenord till din dator när du registrerar dig i konferenser eller liknande på Internet.
- om du får hotelsebrev eller liknande, kontakta din chef. Ta inte bort brevet.
- din e-postadress representerar Emmaboda kommun. Använd den med omdöme.

Observera. E-postsystemet får inte användas för att skicka sekretessbelagd information. E-post är att betrakta som vykort, det kan läsas av en obehörig med rätt kunskap. Skicka därför ingen känslig information via e-post.

INCIDENTER, DATAVIRUS, STÖLD, MM

En incident kan vara i stort sett vad som helst från besökare på villovägar, olåsta dörrar och misslyckad säkerhetskopiering, till driftavbrott, försök till dataintrång och virusangrepp. En incident kan vara en medveten handling eller ske helt oavsiktligt.

Säkerhetsincidenter och brister som kan utgöra ett hot mot säkerheten måste snarast rapporteras. Kontakta närmaste chef och IT-avdelningen om du t ex

- upptäcker svagheter och brister i IT-system/program
- misstänker datavirus, stöld, brand, sabotage etc.

Om du misstänker att någon obehörig använt din användaridentitet och varit inne i IT-systemet ska du:

- notera tidpunkt när du senast var inne i IT-systemet
- notera tidpunkt när du upptäckte intrånget
- omedelbart anmäla till IT-avdelningen och till systemförvaltare samt till din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försök att fastställa om kvaliteten på informationen har påverkats.

DATAVIRUS

Kan beskrivas som ett program eller en programsekvens vars uppgift är tränga in i andra program för att utföra något otillbörligt. Datavirus är ofta ytterst smittsamma och ”smittkällan” kan vara svår att identifiera. Gratisprogram, spelprogram och filer som laddas ner från Internet eller medföljande filer till e-post är vanliga smittbärare. Även besök på webbsidor med tvivelaktigt syfte kan medföra virusangrepp.

Emmaboda kommun har bra programvaror för viruskontroll och det görs kontinuerligt kontroll i nätverket, men det tillverkas hela tiden nya datavirus så det gäller att du är vaksam.

Tecken på datavirus i systemet kan vara att:

- datorn utför operationer/arbete utan att du själv initierat det.
- datorn uppträder på ett onormalt sätt, t ex arbetar mycket långsamt.

Tyvärr är moderna virus så gott som omöjliga att upptäcka om inte virusskyddet larmar. Om du misstänker att systemet innehåller virus ska du:

- INTE stänga din dator genom att slå av strömmen utan istället dra ur nätverkskabeln och stänga av det trådlösa om det finns.
- omedelbart kontakta IT-avdelningen.

Om du får brev med virusvarning där man talar om att ett virus är på gång ska du inte skicka meddelandet vidare. Vid osäkerhet kontakta IT-avdelningen som kan avgöra om det är en seriös varning eller kanske bara ett skämt.

FELAKTIG ANVÄNDNING AV IT

Användning av informationsteknik som tillhandahålls av Emmaboda kommun, t ex datorer, läsplattor och telefoner, ska i huvudsak vara arbetsrelaterad.

Vid sammanträden gäller självklart god mötesordning, dvs man använder sin(a) enhet(er), dvs datorer, läsplattor och telefoner mm, till det som är tänkt att de ska användas till och telefonerna skall vara bortkopplade och/eller i tyst läge. Att sitta och tex surfa på sidor, läsa privata mail eller vara upptagen med sådant som inte tillhör sammanträdet skall man inte göra.

All misstanke om brott ska polisanmälas.

När det gäller elever och anställdas nyttjande beslutar IT-chefen om granskning av loggar. Granskning sker efter begäran från polis, kommunchef, förvaltningschef eller VD. För utredning av elevers nyttjande kan begäran komma från rektor. Resultatet av granskningen lämnas till den som begärt granskningen.

Utöver ovanstående beslutade granskning ska inte IT-avdelningen aktivt kontrollera att användare följer informationssäkerhetspolicyn och dess säkerhetsinstruktioner. Om IT-tekniker ändå upptäcker felaktig användning ska IT-chefen omedelbart underrättas. IT-chefen avgör därefter vilken åtgärd som ska vidtas och om polisanmälan ska göras. IT-chefen ska alltid underrätta ansvarig chef eller rektor. Ansvarig chef avgör om arbetsrättsliga åtgärder ska vidtas.

FÖRVARING OCH HANTERING AV UTRUSTNING

Dina enheter ska föravaras och hanteras på ett sådant sätt att endast behöriga har åtkomst till det arbetsrelaterade innehållet. Den fysiska hanteringen ska ske på ett så omsorgsfullt sätt att vi får en långsiktig hållbarhet.

ÖVRIGT

STÖD OCH HJÄLP

Kontakta IT-avdelningen via helpdesk eller på anknytning 49025 när du behöver hjälp eller har någon fråga om säkerhet eller användning.

NÄR DU SLUTAR DIN ANSTÄLLNING

Ansvarar du för att

- rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas. Notera att allt arbetsmaterial du framställt anses vara kommunens egendom och får inte tas med utan chefs godkännande.
- privat material rensas och tas bort.

De behörigheter du fått i våra IT-system avbeställs genom din chefs försorg.