HÖGSBY
KOMMUN

Informationssäkerhetsinstruktion: Användare (Infosäk A)

Dokumenttyp	**Dokumentnamn** Infosök A Högsby.doc	**Beslutad/Antaget** 2010-09-06 KF §130	**Version** 1.0
Dokumentägare Kommunstyrelsen	**Dokumentansvarig** IT-strateg	**Reviderad**	**Giltighetstid** 2010-

0 Sammanfattning

Datorerna på Högsby kommun är ett arbetsredskap som Du som användare får tillgång till för att underlätta ditt arbete. ***Varje enskild användare ansvarar för att resurserna används professionellt, etiskt och enligt lag*.** Här hittar du regler och rekommendationer som du ska följa när du hanterar information digitalt. Det är viktigt att alla respekterar dessa regler för att kommunen ska kunna behålla allmänhetens förtroende för en säker hantering av deras ärenden. Det är respektive chef som ansvarar för att dessa regler efterlevs.

Utöver den användarinstruktion du nu läser finns ytterligare ett antal dokument som styr informationssäkerhetsarbetet, bl a ett som vänder sig till förvalningschefer/systemägare och ett som reglerar IT-avdelningens ansvar. (Kap 1)

Det finns många aspekter av informationssäkerhet. Du förväntas känna till dem som berör din roll. Andra medarbetare har andra roller i säkerhetsarbetet. (Kap 2)

Säker informationshantering innebär att bara den som har behörighet ska kunna se eller ändra informationen. Behörigheten styrs av inloggningar, som kan liknas vid in-passage till olika informationsrum där ditt konto + lösenord normalt är nyckeln för att låsa upp dörren. Ju säkrare nyckelsystem t ex inloggningskort, dosa desto svårare blir det för den obehörige. (Kap 3)

I den digitala världen lurar andra faror än dem vi är vana vid. Skadlig programvara, felaktigt installerade program, felaktigt lagrad information mm kan ge förödande konsekvenser. Därför finns regler för hur du som användare får nyttja de datorresurser som ställts till ditt förfogande. Läs mer om hur du skyddar din arbetsplatsutrustning och dess information i kapitel fyra. Vad gäller för bärbara datorer? Mobiltelefonen? USB-minnet? Får rumsgrannen låna min dator? Vad gör jag med en utbytt och skrotad dator? (Kap 4)

Lär dig var du ska lagra information i kapitel fem. Det finns skäl att fråga sig vem som ska kunna se, ändra eller ta bort information. Lär dig att spara på rätt plats så förhindrar du att informationen hamnar i orätta händer. Du bör också känna till vad som gäller för allmänna handlingar och vilka lagar som styr personuppgifter mm. (Kap 5)

I kapitel sex och sju tas användningen av Internet och e-post upp. Hur undviker du att drabbas av farorna som lurar vid digital informationssökning och kommunikation, utan att gå miste om de fantastiska möjligheter som erbjuds? Får man ladda ner filer från nätet? Vad skiljer e-post från vanlig post? Vem kollar upp var jag surfar? (Kap 6-7)

Om olyckan är framme och du misstänker att något är galet, att vi fått in virus i våra system, att någon tagit över din dator eller olovligt kommit åt information, ska du alltid rapportera till din chef eller direkt till IT-avdelningen! (Kap 8)

När någon slutar är det viktigt att tänka på en säker avveckling av behörigheter och att någon tar hand om ditt arbetsmaterial. (Kap 9)

Instruktionen avslutas med tips om vart du kan vända dig om du har frågor (Kap 10) och

en bilaga som förklarar klassningsmodellen.

1 Styrande dokument

Styrande dokument för informationssäkerhetsarbetet är Högsby kommuns informationssäkerhetspolicy och informationssäkerhetsinstruktionerna Förvaltning, Kontinuitet och Drift samt den du just läser, Användare.

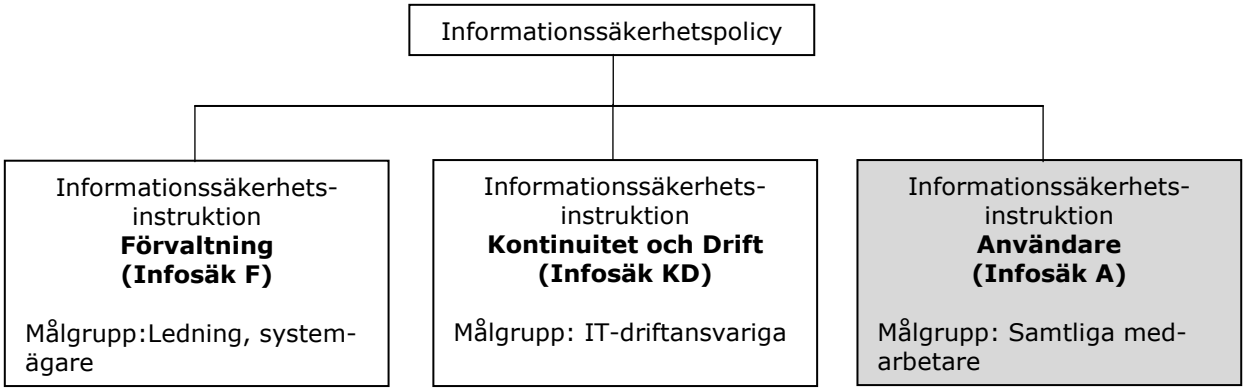

Bild 1 Styrande dokument

Informationssäkerhetsinstruktion Användare (**Infosäk A**) redovisar hur en användare ska verka för att upprätthålla en god säkerhet.

Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

- organisation och roller för informationssäkerhetsarbetet.
- krav på riktlinjer för områden av särskild betydelse.

Informationssäkerhetsinstruktion Förvaltning (**Infosäk F**) redovisar:

- det ansvar som ingår i de olika rollerna.
- de riktlinjer som gäller för områden av särskild betydelse.
- regler för systemutveckling, systemunderhåll, incidenthantering.

Informationssäkerhetsinstruktion Kontinuitet och Drift (**Infosäk KD**) redovisar:

- organisation och ansvar för drift av informationssystemen.
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering som baseras på IT-systemens krav.

Gällande dokument återfinns på kommunens intranät under Styrande dokument.

2 Användarens ansvar (organisation och roller)

Information är en viktig tillgång för Högsby kommun. För att skydda denna krävs ett säkerhetsmedvetande hos alla medarbetare. Som användare har du alltså en del i ansvaret för säkerheten i informationshanteringen. Men du är inte ensam. Så här organiseras informationssäkerhetsarbetet.

Det övergripande ansvaret för kommunens IT-system vilar på kommunstyrelsen. Kommunchefen utser systemägare för vart och ett av kommunens IT-system.

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. Systemägaren är registeransvarig, ser till att informationen följer gällande lagstiftning, avgör vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen, mm. Beslutar om behörigheter.

Systemförvaltare – Operativt ansvarig och utsedd av systemägaren, är den person som har ansvaret för den dagliga användningen av IT-systemet (t ex Extens, Heroma,Castor), hanterar behörigheter och har kontakt med leverantören i frågor om systemets funktion. Systemförvaltare samverkar med IT-avdelningen för att säkerställa en säker och rationell drift av systemet.

IT-ansvarig - IT-ansvarig, för närvarande kommunchef, är övergripande ansvarig för hela IT-verksamheten och för IT-säkerhetsfunktionen som ingår i denna verksamhet samt för IT-verksamhetens budget och ekonomisk uppföljning. IT-ansvarig understödjer arbetet med att uppnå målen i *Informationssäkerhetspolicyn*.

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

Systemtekniker - tillhör IT-avdelningens driftsgrupp. Gruppen innehar den tekniska kompetensen och ansvarar tillsammans med systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-strateg.

Användare - varje användare ska följa gällande regler för informationssäkerhet. I detta ansvar ingår att

- delta i och stödja informationssäkerhetsarbetet
- noga ta del av och följa *Informationssäkerhetsinstruktion Användare*
- rapportera olika former av fel, brister och incidenter, t ex misstänkt virusangrepp
- påtala egna behov av utbildning

För stöd och hjälp när det gäller användningen av verksamhetens program kontaktar du aktuell systemägare/systemförvaltare, se länk:
http://bubblan.hk.hogsby.se/dator_verksamhetsprogram
Har du problem med din datorutrustning, kommunikation, utskrifter etc ska du kontakta IT-avdelningen. Se kap 10 Stöd och hjälp.

Informationssäkerhetssamordnare – länsgemensam resursperson anställd av regionförbundet. Ansvarar för samordning, stöd/utbildning och uppföljning.

Det står mer om de olika rollernas ansvar i *Informationssäkerhetsinstruktion Förvaltning*.

3 Åtkomst till information

3.1 Behörighet

Våra olika informationssystem 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, skriftligt kvitterat att du tagit del av broschyren ”Viktig info om känslig info”.
- att du fått information om säkerhetsaspekterna för de informationssystem du kommer att använda.

Behörighet utdelas normalt som ett lösenord kopplat till ett användarnamn, men vissa informationssystem kräver säkrare identifieringskontroller som lösenordsdosor eller säkra kort. Alla behörigheter ska betraktas som utkvitterade nycklar.

3.1.1 Åtkomst till kommunens lokala nät

Nästan alla som arbetar i vår organisation ges behörighet till våra lokala nätverk och en personlig brevlåda för elektronisk post. Åtkomst till det lokala nätverket ger bl a tillgång till central lagring av dokument, gemensam utgång till Internet, nätverksskrivare och centralt lagrade program. Följande gäller avseende det lokala nätverket:

- ***inloggning på nätverket ska ske med din personliga identitet*** (undantag finns för vissa funktioner).
- all inloggning eller försök till inloggning under annan, eller med annans identitet är förbjuden.
- när du arbetar i kommunens nätverk loggas och registreras 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.
- det är förbjudet att försöka skaffa sig utökade systemrättigheter än dem som tilldelats.

- det är förbjudet att försöka göra utrustning eller information på kommunens nät, åtkomlig utifrån Internet eller annat nät.
- det är förbjudet att skada eller förstöra aktuell information på kommunens nät.
- det är förbjudet att uppenbart slösa med tillgängliga resurser

I normalfallet loggar du in från din ordinarie arbetsplats, en stationär dator eller en tunn klient. Särskilda regler gäller för mobila enheter som bärbara datorer eller avancerade telefoner. Läs mer om dessa i kap 4.

Inloggning via annat nät, t ex via Internet från en dator placerad i hemmet eller i en offentlig miljö, innebär särskilda risker. Du måste känna till att

- arbete utanför kommunens lokaler som kräver uppkoppling mot våra interna nätverk enbart får ske via lösning som tillhandahålls av IT-avdelningen.

Besökande får inte koppla in sin medhavda dator på vårt nät. Undantagna är de sammanträdesrum som har särskilt nätuttag för besökande och de trådlösa gästnät som finns i vissa lokaler.
För besökande, konsulter m fl som behöver låna dator på vårt nät kan IT-avdelningen eller av IT-avdelningen anvisad/godkänd person öppna ett tillfälligt användarkonto som sedan spärras automatiskt.

Undantag från ovanstående kan ske efter samråd med IT-avdelningen.

3.2 Inloggning

Innan du loggar in första gången får du ett lösenord för åtkomst till vårt lokala nätverk. Lösenordet får du av din närmaste chef eller av chefen anvisad person. ***Du måste byta till ett personligt lösenord direkt efter första inloggningen*** (tryck ctrl-alt-del när du är inloggad på datorn). Liknande förfaranden gäller för de enskilda verksamheternas informationssystem som kräver lösenord för åtkomst. Oftast får du sådana lösenord av systemförvaltare eller liknande på din avdelning/förvaltning.

Lösenord är strängt personliga och ska hanteras därefter. Du lämnar spår efter dig när du är inloggad och arbetar i systemen.

- Lösenord får inte skrivas ner och förvaras tillsammans med kontonamnet, eller där det är åtkomligt för obehöriga.
- Lösenord får inte röjas för någon.
- Använd **aldrig** något av dina skarpa nätverkslösenord vid inloggning till resurser på Internet.

Efter fem misslyckade försök att logga in spärras ditt konto. Spärren försvinner efter 30 minuter.

Har du glömt ditt lösenord tilldelas du ett nytt lösenord av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person.

3.3 Val av lösenord

För lösenord gäller för närvarande att det:

- ska vara minst sex tecken långt.
- ska vara komplext och bestå av en blandning av stora och små bokstäver, siffror och specialtecken.
- inte får återanvändas.

3.4 Byte av lösenord

Byte av lösenord

- till våra lokala domäner krävs var 90:e dag. En dialogruta visas på skärmen när det är dags.
- för åtkomst till andra system sker med tidsintervall som bestäms av respektive systemägare.
- ska göras omedelbart och på eget initiativ om du misstänker att någon annan känner till lösenordet.

Kommunens lösenordsprinciper kan komma att förändras löpande.

4 Din arbetsplats

4.1 Stationära datorer och terminaler (tunna klienter)

Följande säkerhetsregler gäller för din datorarbetsplats med tillhörande utrustning:

- Datorn ska vara ID-märkt och stöldskyddsmärkt.
- Fysiska ingrepp får endast utföras av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person.
- Fel ska omgående anmälas till IT-avdelningen via IT-Helpdesk.
- All installation och konfiguration får endast utföras av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person. Gäller t ex anslutning av mobiltelefonbrygga eller kortläsare. Om du är i behov av ytterligare hårdvara ska du ta upp detta med din chef som kontaktar IT-avdelningen.
- Din arbetsplatsutrustning är kommunens egendom och får inte bytas, förändras eller tas med utan IT-avdelningens och verksamhetschefens medgivande.
- Placera alltid din skärm så att den inte kan läsas av andra i rummet eller från fönstret.

4.2 Bärbar dator

Utöver de regler som gäller för stationära datorer gäller särskilda säkerhetsregler för dig som använder en personlig, bärbar tjänstedator:

- Du ansvarar personligen för att datorns installerade säkerhetsprogram är aktiva och uppdaterade. Exempel: antivirusprogram, brandvägg och säkerhetsuppdateringar.
- Du bör inte lämna datorn utan uppsikt, t ex i bilen eller på allmänna platser.

Särskilda regler gäller för lagring på bärbar dator, se kapitel 5.

4.3 Annan mobil utrustning

- Det är inte tillåtet för användare att ansluta mobila enheter till kommunens lokala nät. Kontakta din chef eller IT-avdelningen om du har ett behov av detta.
- Mobiltelefoner får endast kopplas in på kommunens lokala nät med hjälp av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person. Med inkoppling avses anslutning av telefonen via USB-kabel, BlueTooth, IR eller särskild vagga, men också synkroniseringskonfiguration där mobiltelenätet (NMT/GSM/GPRS/Edge/3G osv) används.
- Efter att IT-avdelningen konfigurerat en säker anslutning får denna bara användas för ursprungligt syfte, t ex synkronisering av e-post eller överföring av digitalfoton.
- Anslut inte mobil kringutrustning till en dator som du inte med säkerhet vet har ett uppdaterat antivirusprogram.

Särskilda regler gäller för lagring på mobila enheter. Se kap 5.

4.4 Service på utrustning

Inför service på din utrustning som lämnas bort utanför kommunens egen organisation ska känslig information tas bort eller krypteras. Detta är särskilt viktigt när det gäller bärbara datorer, där lagring på lokala diskar kan vara aktuell. Rådgör då med din chef eller kontakta IT-avdelningen för hjälp.

4.5 Anskaffning och avveckling av utrustning

IT-avdelningen ska alltid anlitas vid inköp av datorutrustning och tillbehör så att den utrustning som används i kommunen uppfyller gällande säkerhetskrav. Detsamma gäller då du inte längre behöver datorutrustningen eller byter ut den mot modernare utrustning. Informera din chef som kontaktar IT-avdelningen för anvisningar om rensning/destruktion.

4.6 När du lämnar arbetsplatsen

Vid tillfällen när du inte har uppsikt över arbetsstationen ska du alltid låsa arbetsstationen eller logga ut. Vid slutet av arbetsdagen ska du logga ut och stänga av datorn. En

avstängd dator drar mindre energi, och försvårar intrång. Vissa säkerhetsuppdateringar aktiveras endast vid omstart eller inloggning.

4.7 Upplåtelse av datorarbetsplats

- Du får aldrig låta någon annan använda din arbetsplats utan att först logga ut. Undantag kan göras för IT-avdelningens personal eller av IT-avdelningen anvisad/godkänd person.
- För att en besökare/leverantör ska få nyttja kommunens datorarbetsplatser måste tillfälliga konton utfärdas av IT-avdelningen eller av IT-avdelningen anvisad/godkänd person.
- Innan du tillåter anslutning av främmande USB-enhet eller liknande till din arbetsplats ska innehållet skannas av antivirusprogrammet. Kontakta IT-avdelningen om du är osäker.

4.8 Programvaror

- Programvaror ska installeras av IT-avdelningen eller av IT-avdelningen anvisad/god-känd person.
- Egna program får inte installeras i Högsby kommuns datorer, oavsett om du har licensrätt eller ej (piratkopierade program). Ej heller s k fria program, nedladdade från Internet. Kontakta alltid IT-avdelningen om du uppmanas att installera ett program, en plug-in, en ActiveX-komponent e dyl.
- Uppdateringar av redan installerade och godkända program kan i vissa fall utföras av dig själv. Det gäller framför allt Windows- och antivirusuppdateringar, men antalet kan komma att utökas.
- Det är inte tillåtet att kopiera eller använda Högsby kommuns program utanför vår verksamhet.
- Om du är i behov av ytterligare programvaror ska du anmäla det till din chef, som kontaktar IT-strateg för inköp/installation.

5 Hantering av information

5.1 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 och säkert 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.

Tystnadsplikt omfattar alla uppgifter man får tillgång till i tjänsten, såväl muntliga som skriftliga. Tystnadsplikten gäller även efter att du slutat din anställning.

5.2 Allmän handling

Handlingar kan vara allmänna eller icke allmänna (t.ex. arbetsmaterial). Allmänna handlingar kan sedan vara offentliga eller sekretessbelagda. Allmänna handlingar måste registreras och arkiveras. Det gäller även handlingar som kommer in via fax eller e-post. Denna instruktion är en allmän handling. En begäran om allmän handling ska åtgärdas skyndsamt. Det innebär att du alltid kan ta den tid du behöver för att fråga om råd. Om du är tveksam ska du kontakta din chef.

Handlingar är inte allmänna om de:

- är minnesanteckningar, det vill säga hör till ett ärende utan att tillföra ärendet sakuppgifter
- utväxlas som arbetsmaterial under ett ärendes beredning
- är myndighetsinterna meddelanden och informationsmeddelanden
- tas emot av en person i egenskap av annan ställning, till exempel partipost till politiker eller post till facklig förtroendeman
- är rent personliga meddelanden i ett meddelandesystem

Huvudregeln är att allmänna handlingar är offentliga, men ibland sekretess-belägger man t.ex. för att skydda den enskilde. Sekretessen bedöms från fall till fall. Arbetsmaterial som inte har arkiverats (handling som inte har färdigställts) är normalt inte allmän handling och behöver inte lämnas ut även om någon begär det. Sekretess som rör rikets säkerhet ska hanteras enligt särskild instruktion och får aldrig lagras i nätverket utan ska lagras på dator eller hårddisk som låses in i säkerhetsskåp. Ta reda på av din chef vad

som gäller just för din verksamhet.

I PUL (personuppgiftslagen) regleras hur man behandlar personuppgifter för att undvika kränkning av den enskildes integritet genom behandlingen av personuppgifterna.

Tänk efter vad du lagrar eftersom man aldrig kan vara helt säker på att ingen obehörig får tillgång till den information som finns där. T.ex. kan intrång i nätverket ske. Spara inte information som kan tänkas vara sekretessbelagd på lokal hårddisk c:. Spara istället informationen på H:\ som antingen lösenordsskyddad (finns som funktion i ordbehandlings-program) eller genom kryptering, IT-avdelningen har program för det.

För mer information, se www.riksdagen.se:
Tryckfrihetsförordningen (TF)
Förvaltningslagen
Kommunallagen
PUL – Personuppgiftslagen
Sekretesslagen

5.3 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 kommunens personuppgiftsombud i ett tidigt stadium i planeringen av registret.

En annan lag som ställer krav på de informationsbehandlare som arbetar med sjukvård är Patientdatalagen. Här gäller särskilda krav på autentisering och spårbarhet.

5.4 Klassning av information

Informationssystem inom Högsby kommun klassas utifrån den information som hanteras i systemet. Klassning görs från aspekterna sekretess (konfidentialitet), riktighet och tillgänglighet.

Sekretess:	Att informationen skyddas från obehörig insyn.
Riktighet:	Att informationen inte ändras på ett obehörigt sätt.
Tillgänglighet:	Att informationen finns tillgänglig för rätt person vid rätt tillfälle.

Tas information ut ur systemet och lagras på andra media, eller används i ett annat sammanhang, måste den klassas där den används och hanteras därefter.

Även information i arbetsmaterial måste klassas.

Innan du lagrar eller hanterar dokument bör du alltid fråga dig:

- Vem ska kunna se informationen?
- Vem ska kunna ändra informationen?
- Var bör informationen lagras?

Högsby kommuns klassningsmodell framgår av bifogad bilaga.

5.5 Lagring av information

Det finns två olika typer av lagring.

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.

När du arbetar i ett sådant system har du alltså fått hjälp med klassningen av bl.a. systemägaren.

IT-avdelningen svarar för att automatisk säkerhetskopiering genomförs av databaser och programkataloger för respektive verksamhetssystem.

Egna register/dokument
Utöver att arbeta i våra verksamhetssystem kommer du 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 måste själv 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.
- Du måste känna till de regler som gäller för gallring av information.

Gallring är en strukturerad utrensning av information som enligt lag bedöms vara mindre betydelsefull i ett långtidsperspektiv.

Det innebär att gallring alltid ska föregås av informationsklassning där informationens värde bestäms utifrån krav från lagstiftning och verksamhet. Idag produceras mer information än någonsin på olika medier, därför blir också gallringen allt viktigare eftersom icke väsentlig information tynger informations-systemen.

I den offentliga verksamheten styrs gallring från tryckfrihetsförordningen och arkivlagen som innebär att en mycket stor del av den information som inkommer till Högsby kom-

mun är att betrakta som allmänna handlingar. Allmänna handlingar får inte förstöras utan ett gallringsbeslut. Detta gäller även e-post, cookie-filer och temporära Internet-filer (Globalfiler). Idag sparas cookie-filer och Globalfiler lokalt på varje dator utifrån standardinställningar i aktuell webbläsare.

5.5.1 Lagring på administrativt nätverk

Den information du lagrar på våra gemensamma lagringsutrymmen säkerhetskopieras automatiskt. Du kan välja att lagra på enheterna G:, T:, eller H:

G: (Gemensam gruppenhet) är en enhet för lagring av information som alla medarbetare i organisationsgruppen har tillgång till. Enheten används när man vill dela information mellan kollegor inom en avdelning eller förvaltning.

T: (Offentlig enhet, Tunnan) är en enhet för lagring av information som alla i organisationen kan ta del av. Var och en ansvarar för att rensa bort informationen efter sig.

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.

Ytterligare enhetsbeteckningar kan vara tillgängliga, men de ovanstående ska alla känna till och förstå syftet med.

Om du lagrar på din lokala hårddisk (C: eller D:) är du personligen ansvarig för säkerhetskopiering. När du lagrar information på din lokala hårddisk (C: eller D:) riskerar du att förlora information som inte kan återskapas till rimliga kostnader, vid t ex en diskkrasch. Undvik därför att lagra viktig verksamhetskritisk information på lokala diskar.

5.5.2 Lagring på utbildningsnätverk

Den information du lagrar på våra gemensamma lagringsutrymmen säkerhetskopieras automatiskt. Du kan välja att lagra på enheterna T:, R. eller H:

T: (Offentlig enhet, Tunnan) är en enhet för lagring av information som alla i organisationen kan ta del av. Tunnan ses av både elever och personal

R: (Offentlig enhet, Arkiv) är en enhet för lagring av information som all personal inom skolan kan ta del av. Undermapparna nås av respektive skolenhet.

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.

Ytterligare enhetsbeteckningar kan vara tillgängliga, men de ovanstående ska alla känna till och förstå syftet med.

Om du lagrar på din lokala hårddisk (C: eller D:) är du personligen ansvarig för säkerhetskopiering. När du lagrar information på din lokala hårddisk (C: eller D:) riskerar du att förlora information som inte kan återskapas till rimliga kostnader, vid t ex en diskkrasch. Undvik därför att lagra på lokala enheter.

5.5.3 Lagring på mobila enheter

Mobila lagringsenheter kan vara fristående:

- disketter, CD-skivor, DVD-skivor, USB-minnen, fristående hårddiskar etc

eller integrerade:

- hårddisken i en bärbar dator, det interna minnet i en PDA eller mobiltelefon, en MP3-spelare eller en digitalkamera och de löstagbara minneskorten till dessa.

Alla dessa portabla lagringsenheter kräver särskild uppmärksamhet ur ett informationssäkerhetsperspektiv.

5.5.4 Lagring på bärbar dator

Om du använder en personlig bärbar tjänstedator för arbete utanför kommunens nätverk ska du tänka på att den utsätts för större risker och att du därför inte får lagra sekretessbelagd eller för verksamheten känslig information på den.
Följande gäller för lagring av information på bärbar dator:

- Kryptering ska användas om det finns risk för obehörig åtkomst till informationen.
- Du är ansvarig för att datorn har ett uppdaterat skydd mot skadlig kod.
- Innan du kopierar in data till din bärbara dator ska filerna skannas för att upptäcka skadlig kod.
- Kontrollera med din chef om det är tillåtet att kopiera informationen till flyttbart media som du sedan t ex tar med hem.
- Du är själv ansvarig för att information lagrad på den bärbara datorn säkerhetskopieras.
- Om offline-hantering är aktiverad bör du kontinuerligt kontrollera att ingen information går förlorad vid synkroniseringen, och att all viktig information säkerhetskopieras.

5.5.5 Lagring i mobiltelefonen

Din mobiltelefon har inte samma skyddsmekanismer som en bärbar dator. Den saknar oftast brandvägg, virusskydd och krypteringsmöjlighet. Även om du har låskoder på telefonen så kan en obehörig ändå plocka ut minneskortet och läsa det i en annan telefon.

- Därför ska du inte lagra verksamhetsinformation på din mobil. Radera regelbundet e-post, bilagor och övriga dokument från din mobiltelefon sedan du lagrat undan dem på arbetet.
- Aktivera låskoden för telefonen och kryptera data om telefonen medger det.
- Lämna aldrig mobiltelefonen obevakad – den är stöldbegärlig.
- Installera aldrig program skärmsläckare utan att rådfråga IT-avdelningen.

- Aktivera inte öppen Bluetooth eller IR så att enheten aviseras för andra BT/IR-enheter.

5.6 Utskrifter

Utskrifter av känslig eller sekretessbelagd information på gemensamma nätverksskrivare kräver särskild försiktighet. För att skriva ut sådan information måste skrivaren antingen ha autentisering via personlig kod, eller vara otillgänglig för obehöriga i ett låst utrymme.
Skrivarens lagringsarea ska vara skyddad för obehörig åtkomst.
Inga utskrifter får ligga kvar i skrivaren. Utskrifter ska hämtas snarast.

6 Nätverk

6.1 Regionnätet ”regneth”

Vissa informationssystem utnyttjar vårt länsnät, regneth. Det kan gälla arbete i bibliotekssystem, skolhälsovårdssystem, vårdjournaler mm. Som användare bör du vara medveten om att dessa system kan omfattas av andra organisationers säkerhetsregler. Systemägaren/systemförvaltaren kan lämna mer information om detta.

6.2 Internet

När du använder Internet kan säkerheten i Högsby kommuns lokala nätverk påverkas negativt beroende på ditt beteende. Kommunen förutsätter att den som från sin arbetsplats surfar eller laddar ner filer från Internet har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välkända och seriösa 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 för brott mot upphovsrätten.

Kanske använder du Internet för att komma åt viktiga resurser hos någon leverantör. Då är det extra betydelsefullt att skydda och säkra sin inloggning, eftersom hela världen har tillgång till Internet.

- Spara inte inloggningsinformationen på din dator om du får en sådan fråga.
- Använd **aldrig** något av dina skarpa, lokala nätverkslösenord vid inloggning till resurser på Internet.

Det är inte tillåtet att via Internet titta, sprida meddelanden om 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. Om du är osäker på vad som är tillåtet bör du rådfråga din chef.

Det är inte tillåtet att dela ut datorkapacitet och spela spel över Internet.

Det är inte tillåtet att kommunicera med avsändare inom kommunen där oklarhet kan uppstå om man företräder kommunen eller inte.

Tänk på att du representerar Högsby kommun när du surfar på Internet och att du lämnar spår efter dig i form av Högsby kommuns IP-adresser. Lokal surfhistorik som cookies, temporära filer etc är att betrakta som allmän handling. Det är emellertid tillåtet att gallra dessa efter inaktualitet. Men tänk på att du också lämnar spår på de webbplatser du besöker.

Det är förbjudet att använda någon annans identitet på Internet.

Trafik genom våra brandväggar loggas och vid misstanke om brott studeras loggarna för att spåra vad som hänt. Personalchefen fattar beslut om granskning av loggar om en anställd misstänks, rektor eller motsvarande fattar motsvarande beslut i fråga om misstanke mot elev. Resultatet av granskningen lämnas till den som begärt granskningen.

Kriminell verksamhet polisanmäls.

Förutom vid misstanke om brott kan loggarna analyseras för att kartlägga belastningen på vår internetförbindelse, eller sammanställa icke individualiserad statistik över användningen.

Bedrägerier på Internet sker ofta genom s.k vilseledande webbplatser som liknar originalplatsen. På detta sätt kan man få besökare att ovetande lämna känslig information i felaktiga händer. Om inte krav på identifiering av den som lämnar informationen finns kan man kontrollera att informationen man skickar krypteras (https) och att certifikatets ägare stämmer överens med webbplatsens ägare och att certifikatet inte är för gammalt**.** ***Verkar något misstänkt, lämna webbplatsen utan att lämna någon information.***

6.3 Andra externa nät

Bärbara tjänstedatorer som ansluts till externa trådburna eller trådlösa nätverk som hemmanätverk, hotellnätverk eller andra publika nätverk måste

- ha ett fungerande och uppdaterat antivirusprogram.
- ha den interna brandväggen aktiverad och uppdaterad.

Kom ihåg att arbete utanför kommunens lokaler som kräver uppkoppling mot våra interna nätverk enbart får ske via lösning som tillhandahålls av IT-avdelningen.

7 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. Här presenteras de regler som gäller för användandet av e-post för all personal i Högsby kommun.

E-post är ett rationellt hjälpmedel i arbetet men ska inte användas som lagringsarkiv. Tänk därför på att regelbundet radera i mapparna ”**Inkorgen**”, ”**Skickat**”, och ”**Borttaget**” för att frigöra utrymme så att inte din e-post spärras. Meddelanden, bifogade filer

mm som du vill spara, sparar du på samma sätt som du lagrar annan information.
E-post som ändå lagras i e-postprogrammet ska vara strukturerad och lätt att återsöka.

Förvaltningslagen reglerar vår skyldighet att ta emot e-post från medborgarna samt vår serviceskyldighet att svara skyndsamt. Besvarande av en handling ska ske skyndsamt. Din e-post får därmed inte lämnas oläst och obesvarad under semester, sjukdom eller annan ledighet. Helst skall du kontrollera din egen e-post samt övriga du ansvarar för minst en gång om dagen. Detta gäller även för registrator och ansvariga för myndighets- och funktionsbrevlådor.

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.

Underrättelser av beslut som kan överklagas ska däremot inte skickas via e-post eftersom det då är osäkert att fastställa när parten får del av beslutet.

Du får inte skicka anbudshandlingar per e-post. Anbudshandlingar skall vara undertecknade, och får därmed inte betraktas som inkommet anbud om den enbart kommer via e-post. E-postmeddelandet som sådant skall dock behandlas som vanlig inkommande handling.

E-post med bilagor utgör ett stort hot när det gäller spridning av virus.

- E-postsystemet är ett arbetsverktyg och bör inte användas för privat bruk.
- Samma regler gäller för diarieföring av e-post som för vanliga brev. Du har själv ansvar för bedömningen av din e-post och av den e-post som har vidarebefordrats till dig. Du ska börja med att avgöra om e-postmeddelandet är allmän handling eller inte. Om det är en allmän handling skall handlingen registreras, lämna den till registrator om du inte kan registrera själv. När handlingen är registrerad finns det inte något krav på att du som mottagare av meddelandet ska spara det i din dator.
- Arkivering och aktbildning görs på traditionellt sätt, det vill säga att handlingarna skrivs ut och bevaras som pappershandlingar. Detta gäller både inkommande som utgående handlingar.
- E-post som är allmän handling får gallras, det vill säga raderas, först när e-posten har diarieförts. Om e-postmeddelandet inte är allmän handling får det raderas på en gång. Diarieförda handlingar inklusive e-postmeddelande bevaras/gallras i enlighet med de regler för gallring som framgår av respektive förvaltnings dokumenthanteringsplan.
- Om du misstänker att det kommit in virus via e-postsystemet ska du agera som beskrivits i avsnittet om incidenter, kap 8.
- I e-postsystemet finns en loggningsfunktion som noterar inkommande och utgående meddelanden. Detta innebär att alla meddelanden kan spåras. Vid behov kan logglistan skrivas ut.
- 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.
- Chefer kan begära hos IT-strateg att ge anställd rätt att läsa e-post ställd till en kollega som har semester, är tjänstledig eller är sjuk. Chefen 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 lämnas ut vid begäran. Först ska den dock gallras på eventuell privat e-post och om sekretessbelagda uppgifter skulle ha inkommit.
- Du ska följa de råd om inställningar i och hantering av e-postsystemet som utfärdas av systemägaren eller IT-avdelningen.
- Det är inte tillåtet med automatisk vidarebefordran till extern e-postadress.
- Var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer för att undvika onödig belastning av systemresurser.
- Vid utskick till många interna mottagare bör filer inte bifogas, spara informationen på gemensam katalog och hänvisa dit i brevet.
- Öppna endast bifogade filer från avsändare som du litar på. Var uppmärksam om filtypen på filen stämmer överens med filtyp som ofta används för att sprida virus: .bat, .exe, .com, .vbs, .scr, .pif, .js
- Ange alltid ämne i ämnesraden för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.
- Skriv inte någon känslig information i ämnesraden.
- Kontrollera alltid att adressaten stämmer innan du trycker på Skicka-knappen. Glöm inte att kontrollera vilka som är medlemmar på distributionslistor innan du använder dem (risk att känslig information når fel mottagare).
- Skicka inte och vidarebefordra inte kedjebrev, skämtmail etc.
- Om du får hotelsebrev ska du spara brevet och kontakta din chef.
- Fundera på var 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, sparar eller säljer din e-postadress vilket kan resultera i skräppost.
- Stryk dig från e-postlistor om du inte vill ha fler brev via dem eller om du är frånvarande en längre tid.
- Din e-postadress representerar Högsby kommun. Använd den med omdöme.

Observera. E-postsystemet får inte användas för att skicka sekretessbelagd information

8 Incidenter, virus mm

8.1 Allmänt

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.

Högsby kommun rapporterar IT–incidenter till Informationsäkerhetssamordnare. Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du

- notera när du senast var inne i IT-systemet.
- notera när du upptäckte incidenten.
- omedelbart anmäla förhållandet till IT-avdelningen eller din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på din information har påverkats.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till IT-avdelningen eller din närmaste chef.

8.2 Virus och annan skadlig kod

Högsby kommuns datorer har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av s.k. skadlig kod. Datavirus, maskar, trojaner och annat otyg är ofta ytterst smittsamma och ”smittkällan” kan vara svåra 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 att din dator smittas.

Tecken på skadlig kod i systemet kan vara att

- datorn uppträder på ett onormalt sätt, t ex arbetar mycket långsamt.
- datorn utför operationer/arbete som du inte själv initierat, t ex förändringar sker på skärmen (tecken flyttas, försvinner etc).
- pip eller hälsningar på skärmen.

Tyvärr är moderna skadeprogram så gott som omöjliga att upptäcka om inte virusskyddet larmar.

Om du misstänker att din dator är påverkad av skadlig kod ska du

- dra ut nätverkskabeln, men låta datorn vara på.
- omedelbart anmäla förhållandet till endera IT-avdelningen eller till närmaste chef. OBS! Anmälan ska ske per telefon eller besök, inte per e-post.

Om du får brev med virusvarning där man talar om att ett virus är på gång ska du inte skicka meddelandet vidare. Kontakta IT-avdelningen som kan avgöra om det är en seriös varning eller ett falsklarm, s k hoax.

Handdatorer, digitala kameror, mobiltelefoner mm kan lätt bli virusbärare eftersom du kan lagra information i dessa. Var noga med att den dator du ansluter sådan kringutrustning till har ett uppdaterat virusprogram.

Det är förbjudet att medvetet sprida skadlig kod.

9 Avslutning av anställning

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 Högsby kommuns egendom och får inte tas med utan chefs godkännande.
- privat material tas bort.

De behörigheter du fått för åtkomst till våra informationssystem avbeställs av din chef.

10 Stöd och hjälp

Om du behöver hjälp med din IT-utrustning eller om du undrar över något som gäller informationssäkerhet ska du kontakta IT-Helpdesk.

På kommunens intranät hittar du mer om informationssäkerhet.

Kontaktpersoner

- **Systemägare, Systemförvaltare, Behörighetshandläggare** för respektive program

  se http://bubblan.hk.hogsby.se/dator_verksamhetsprogram

- **IT-Helpdesk / IT-Avdelningen / Systemtekniker**

  Via webb:
  se
  http://bubblan.hk.hogsby.se/intern_service/it_fraagor/felanmaelan_kontakta_it_avd

  Via tfn: 0491-29275

  se http://bubblan.hk.hogsby.se/arbetsplatser/kommunledningsstab/it/personal

- **Stöd till Informationssäkerhetssamordnare / IT-strateg / Behörighetshandläggare för inloggning på dator**

  Tfn: 0491- 29393

  se http://bubblan.hk.hogsby.se/arbetsplatser/kommunledningsstab/it/personal

Bilaga - Klassning av information

1 Information som hanteras i IT-baserade informationssystem

För information som lagras i IT-system måste inte bara sekretessaspekten beaktas, utan även kraven på riktigheten i informationen och tillgängligheten till den.

Säkerhetsaspekt / Kravnivå	Sekretess (konfidentialitet)	Riktighet	Tillgänglighet
Mycket hög nivå	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ska vara åtkomlig inom högst 2 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Hög nivå	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 2 timmar, men inom högst 8 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Basnivå	Information som kan medföra mindre allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra mindre allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 8 timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person

Anm: följande typ av information hanteras utanför klassningsmodellen:

- Information som avser rikets säkerhet. Sådan information ska hanteras enligt särskilda bestämmelser.
- Information som har extrema krav på sig att vara tillgänglig och där utgångspunkten är att den alltid ska vara det.
- Information som inte bedöms ha krav på sig vare sig avseende sekretess (konfidentialitet), riktighet eller tillgänglighet.

2 Information på datamedia

Med datamedia menas magnetiska eller optiska diskar, USB-minnen etc. Dessa medier ska inte ses som slutliga förvaringsformer, såvida de inte avser backuptagning. Information på datamedia är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess (konfidentialitet) beaktas. De krav på sekretess som ställs för ett specifikt IT-system framgår av användarhandledningen för systemet.

För information på datamedia gäller följande krav:

Krav på sekretess	**Åtgärder**
Mycket hög nivå	**Förvaring** – Krypterad på filserver. Applikationsservrar är fråntagna krypteringskravet – Vid förvaring på lokal hårddisk eller annat flyttbart medium ska informationen vara krypterad **Kopiering** – Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån **Överföring** – All överföring ska vara krypterad **Destruktion** – Lämnas till IT-avdelningen för destruktion
Hög nivå	**Förvaring** – På filserver eller applikationsserver – Vid förvaring på lokal hårddisk eller annat flyttbart medium ska informationen vara krypterad **Kopiering** – Får kopieras i samråd med systemets förvaltare/administratör **Överföring** – Kryptering vid överföring utanför organisationen **Destruktion** – - Lämnas till IT-avdelningen för destruktion
Basnivå	**Förvaring** – Inga krav **Kopiering** – Tillåten **Överföring** – Inga restriktioner **Destruktion** – Krävs ej

3 Information på andra media

Med andra media menas papper, film, OH-bilder etc. Information på dessa media är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån. Eftersom informationen är kopierad behöver endast kraven på sekretess (konfidentialitet) beaktas. De krav på sekretess som ställs för ett specifikt IT-system framgår av användarhandledningen för systemet.

För information på ovanstående media gäller följande krav:

Krav på sekretess	**Åtgärder**
Mycket hög nivå	**Förvaring** – Förvaras inlåsta **Kopiering** – Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån **Överföring** – Rek brev eller bud **Destruktion** – Papper och OH-film destrueras i papperstugg
Hög nivå	**Förvaring** – Ej förvaras synligt **Kopiering** – Får kopieras i samråd med systemets förvaltare/administratör **Överföring** – Fax eller brev **Destruktion** – Papper och OH-film destrueras i papperstugg
Basnivå	**Förvaring** – Inga krav **Kopiering** – Tillåten **Överföring** – Inga restriktioner **Destruktion** – Krävs ej