| Regler för IT-säkerhet | | Version 1.2 |
|---|---|---|
| Upprättad av: | Peter Jimmefors | Upprättad: 2012-09-17 |
| Fastställd av: | Johan Fritz | Fastställd: 2012-09-17 |

## Bakgrund

Information är en viktig tillgång för vår organisation. För att skydda de värden informationen representerar krävs ett säkerhetsmedvetande hos alla medarbetare. Du som användare har alltså en del av ansvaret för säkerheten i informations-hanteringen. För att du skall kunna leva upp till de säkerhetskrav som ställs på dig måste du känna till:

- vilket ansvar du har
- vad du skall göra vid olika incidenter
- var du kan få stöd och hjälp

## Helpdesk

IT-enheten har en helpdesk, som nås via intranätets startsida. Det är den primära vägen att anmäla ett fel eller göra beställningar. Skulle det inte vara möjligt att använda denna väg för att komma i kontakt med helpdesken kan mailadressen support@lillaedet.se eller telefonnummer 596 85 användas. Inkomna ärende tas om hand utifrån prioritet och anmälningstid.

## Inloggning

Vårt nätverk är utrustat med ett behörighetskontrollsystem för att säkerställa att det endast är behöriga användare som kommer åt information. För att bli behörig användare krävs din chefs godkännande. Sedan ansvarar Du för att följa de regler som kopplas till behörigheten. IT-enheten ordnar behörighet till nätverk och tillgång till de system som behörig chef beställer. Behörigheter inom respektive system ansvarar systemförvaltaren för.

**För att få behörighet krävs att:**

1. Du ansöker om behörighet hos din chef
2. Chefen beslutar om behörighet till system, vilken anmäls via helpdesken och till systemförvaltaren i god tid.
3. IT-enheten lägger in din behörighet till systemet
4. Därefter får du:
    - en användaridentitet
    - ett lösenord - din egen hemlighet
    - en e-postadress
5. Systemförvaltaren för respektive system lägger upp behörighet i ”sina” system.



| | Adress | Telefon | Telefax | e-post |
|---|---|---|---|---|
| Peter Jimmefors | Järnvägsgatan 12 | 0520-65 95 75 | | peter.jimmefors@lillaedet.se |
| Ekonomiavdelningen | 463 80 LILLA EDET | 0520-65 95 00 | 0520-65 74 20 | kommunen@lillaedet.se |

**Initialt lösenord**
Första gången loggar du in i nätverket med ett initialt lösenord som du får av IT-enheten. Detta lösenord kan du bara använda för att komma in i systemet och byta det till ditt personliga lösenord. Genom detta säkerställs att det är bara du själv som känner till lösenordet.

Lösenordet är strängt personligt och skall hanteras därefter. Du skall därför:

- inte avslöja ditt lösenord för andra eller låna ut din behörighet
- skydda lösenordet väl – alltså ska det inte finnas några nedskrivna lösenord i närheten av datorn.
- omedelbart byta lösenordet om du misstänker att någon känner till det
- byt lösenordet med viss periodicitet, senast vid uppmaning i samband med påloggning.. Vid sex misslyckade påloggningsförsök spärras identiteten och kontakt med helpdesk krävs. Vissa verksamhetssystem kan ha annan periodicitet för lösenordsbyte och spärr.

**Lösenordet skall bestå av minst 7 tecken** och skall konstrueras så att det inte lätt kan kopplas till dig som person. Det måste bestå av minst en siffra och en versal. Enkla repetitiva mönster såsom t ex ”ABC1234”, ”AAAAAA2” skall undvikas, liksom andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller lösenord av typen ”QWERTYU”, dvs. enkla tangentkombinationer.

**Tidigare använda lösenord** kan du inte återanvända. När du byter lösenord kontrollerar systemet att du inte använder något av de lösenord som du tidigare använt.

**Om du glömmer ditt lösenord** vänder du dig till IT-enhetens helpdesk. Du kommer då att få ett nytt initialt lösenord.

**Du lämnar spår efter dig** när du är inloggad och arbetar i systemen. Systemens loggningsfunktion används för att spåra obehöriga intrång. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar. Exempel på det som loggas är vem som är inloggad och när vederbörande loggade in respektive ur systemet samt i viss mån vad den som är inloggad gör i systemet, t.ex. om man skickar e-post loggas tidpunkt, avsändare, mottagare mm för varje försändelse. Olika loggningsfunktioner tillkommer allt eftersom behovet av dessa uppstår.

## Hantering av information

Verksamhetskritisk information lagras på gemensamma diskutrymmen. Sker lagring av annan icke verksamhetskritisk information på lokala arbetsstationer ansvarar Du själv för att denna blir säkerhetskopierad. Om detta inte görs finns risk att informationen försvinner. **För den information du lagrar lokalt på din hårddisk ansvarar du själv, vilket innebär att**

- du själv skall ta säkerhetskopior
- du skall tänka på att andra kan ha otillbörligt intresse av att komma över informationen
- vid en eventuell ominstallation av datorn kommer all information lagrad på lokal disk att raderas

**Internet**

Kommunens lokala nätverk är anslutet till Internet via utrustning, som har möjlighet att loggar in- och utgående trafik. Internetanvändandet är ett område där säkerheten påverkas i mycket hög grad av användarnas beteende. **Vid användande av Internet gäller följande:**

- programvaror av typen shareware, freeware eller liknande får inte laddas ned och installeras eller köras på kommunens datorer utan att de godkänts av verksamhetsansvarig och IT-enheten samt genomgått ett virustest.
  Allmänt gäller att vid nedladdning av filer från Internet krävs att du har gott omdöme och endast hämtar in sådant som är relevant för arbetet och kommer från välrenommerade web-siter.
- Det är inte tillåtet, om arbetet inte så kräver, att via Internet titta/lyssna på material av pornografisk, rasistisk, nazistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, nationalitet etc.) eller har anknytning till kriminell verksamhet.
- När du surfar på Internet representerar du organisationen. Agera i enlighet med våra värderingar så att det du förmedlar på nätet inte skadar oss. Du lämnar spår efter dig i form av kommunens IP-adress.

**Malware (Virus och annan skadlig programvara)**

**Malware** (virus i dagligt tal) kommer av de engelska orden **Mal**icious Soft**ware**, och är ett samlingsbegrepp för datorprogram som installeras på en dator utan administratörens eller användarens vetskap. Det kan vara maskar, virus, trojaner, adware, spyware eller keyloggers. **Ratware** är en annan typ av skadlig kod, som används för att skapa massutskick av skräppost över Internet.
Ofta innehåller den skadliga programvaran kod för att leta rätt på e-postadresser på den drabbade datorn och skicka koden vidare till dessa. För att göra meddelandet mer personligt kan en del virus använda dokument eller dokumentfragment de hittar på datorn.

Spridning av virus sker ofta genom e-post och då oftast i form av en bifogad fil eller en länk i själva meddelandet. Är avsändaren okänd och/eller du inte vet vad det är du fått är tumregeln att inte öppna bifogade filer eller klicka på länkar. Är du oförsiktig i det här läget kan du lätt komma att köra koden och datorn kan då bli smittad. Ibland utnyttjas svagheter i operativsystemet eller e-postprogrammet så att koden körs mer eller mindre automatiskt. Internetsidor med ”tvivelaktigt” innehåll kan också vara en källa för virus och du bör ha detta i åtanke när du surfar från en av kommunens datorer.

Det är idag svårt att veta om du har virus i datorn och det är inte ovanligt att användaren inte märker något alls av att datorn är smittad. För att i den mån det är möjligt förhindra detta har samtliga datorer i verksamheten ett antivirusprogram installerat, detta inget du som användare märker av utan det sköts och administreras centralt från IT-enheten och normalt märker du bara av antiviruset när det har hittat ett virus och varnar för detta. .
När du misstänker att du har fått virus i datorn eller när du får en virusvarning skall du genast sluta använda datorn och direkt kontakta helpdesk. Datorn får efter detta inte användas förrän IT-enheten gett klartecken på att den är ”ren” från virus/malware.
Nedan följer en kort förklaring av dom vanligaste varianterna av Malware.
**Virus** - Sprider sig till filer lagrade på den infekterade datorn och följer med infekterade filer när de överförs till andra datorer.

**Mask/Worm** - Sprider sig via datornätverk mellan datorer och allt som oftast utan inblandning från en användare.
**Trojansk häst/Trojan** - Utger sig för att göra en sak, men utför andra saker vanligen dolda för en användare, t.ex nedladdning av spionprogram, skicka spam mm.
**Logisk bomb** - Utför en (skadlig) handling under speciella villkor, till exempel att ett visst datum infinner sig.
**Spionprogram/Spyware** - Spionerar på privat information på infekterade datorer, och skickar informationen över internet.
**Annonsprogram/Adware** - Visar annonser på infekterade datorer.
**Keylogger** - Registrerar information om de tangenter som trycks på datorn, till exempel lösenord, och lagrar informationen lokalt för senare åtkomst eller skickar den via internet.

## E-post

E-post är ett rationellt hjälpmedel i arbetet. Med tiden sparar man kanske på sig stora mängder meddelanden som ofta innehåller bifogade filer. Tänk därför på att regelbundet radera i din inkorg och använda de verktyg som finns för att tömma papperskorgen. Kommunen har ett spamfilter som filtrerar det mesta av skräpposten som kommer, men det händer även att ”riktig” post hamnar där. Om du saknar något eller vill kontrollera filtret så kan du få tillgång till din egna spambrevlåda – kontakta i så fall Heldesk.

**För att undvika problem med ökad risk för virusspridning och onödig belastning av systemresurser:**

- var selektiv med att skicka eller vidarebefordra meddelanden som innehåller stora filer. Bilder, PowerPoint-presentationer med mycket grafik och liknande är generellt utrymmeskrävande
- öppna endast bifogade filer från avsändare du litar på, vid osäkerhet kontakta helpdesken i händelse av att spamfiltret inte har stoppat suspekt e-post.
- meddelande där du blir uppmanad att skicka en kopia till alla i din adressbok raderas utan åtgärd då dessa endast har till uppgift att generera stora mängder e-posttrafik
- Om du misstänker att det kommit in virus via e-postsystemet skall du agera som beskrivits i avsnittet om Internet.

Möjligheten att använda webmail finns också. Om inloggning till webmail sker från en offentlig dator (t.ex. på ett bibliotek) måste du logga ut från webmailen och webläsaren stängas innan du lämnar datorn. Om mail synkroniseras med telefonen måste PIN-kod finnas för att logga in på telefonen likväl som till SIM-korten (alltså krävs två inloggningar för att använda telefonen).

## Incidenter

Om du misstänker att någon obehörig använt din användaridentitet

- notera tidpunkt då du senast själv var inloggad
- notera tidpunkt då du upptäckte förhållandet
- anmäl omedelbart till din chef
- dokumentera alla iakttagelser i samband med upptäckten samt försök att fastställa om kvaliteten på informationen har påverkats

Om du misstänker datavirus

- kontakta helpdesk (se i övrigt avsnitt om virus och annan skadlig programvara)

Om du misstänker stöld, brand, sabotage etc.

- kontakta närmaste chef

**Bärbar utrustning och lagringsmedia**

Bärbara persondatorer, surfplattor, smartphones och lagringsmedia som du använder utanför din ordinarie arbetsplats utgör en säkerhetsrisk. Därför bör du:

- hålla utrustning och lagringsmediamedia under ständig uppsikt om du inte kan låsa in den
- tänka på att du inte får lagra verksamhetskritisk information på den bärbara utrustningen eller lagringsmediet
- förvara en säkerhetskopia av all information på din ordinarie arbetsplats
- alltid hantera utrustningen så att stöld försvåras i möjligaste mån, till exempel genom att låsa fast den bärbara datorn med vajerlås

**Arbetsplatsen**

Om du lämnar arbetsplatsen skall du alltid låsa arbetsstationen alternativt logga av, även om det bara är för en kortare stund. Om du glömmer detta kommer arbetsstationen att vara tillgänglig för obehöriga till det att skärmsläckaren startas och automatiskt låser arbetsstationen. Kom ihåg att du ansvarar för allt som registrerats med din användaridentitet. För att låsa arbetsstationen trycker du ”Ctrl+Alt+Delete” och väljer ”Lås datorn” alternativt tangentbordets ”windowsknapp + L”. För att låsa upp arbetsstationen trycker du ”Ctrl+Alt+Delete”, skriver in ditt lösenord och trycker på ”Enter”. Datorn ska också stängas av när du lämnar arbetsplatsen för dagen, det räcker alltså inte med att stänga av bildskärmen, så att eventuella uppdateringar kan genomföras på ett säkert sätt.

**Utskrifter av dokument**

Utskrifter ska ske sparsamt och om möjligt på nätverkskopplade skrivare. Utskrifter ska inte lämnas i skrivaren då dokument kan komma i orätta händer.

**Problem med utrustning**

Successivt kommer ett internleasingförfarande att införas i kommunen, där IT-enheten äger utrustningen och respektive verksamhet leasar den. Alla problem ska felanmälas till helpdesken som beslutar om åtgärd.

**Stöd och hjälp**

Beroende på vilken typ av problem som uppstår så ska du söka hjälp på olika håll.

- Om ett verksamhetssystem inte fungerar som det ska eller förändring i behörighet önskas kontaktas systemförvaltaren.
- Handhavandeproblem i övriga programvaror löses främst genom att rådfråga en annan kollega. Först därefter kontaktas helpdesken.
- Problem med kommunikation, inloggning till nätverk mm anmäls till helpdesken.
- IT-enheten har en helpdesk som loggar anmälda ärenden och dessa tas omhand efter prioritet och anmälningstid.

**Andra kopplade dokument:**

- Riktlinjer för IT i Lilla Edets kommun, dnr 2009/KS0203
- Rollfördelning över IT-system i Lilla Edets kommun