



# IT- säkerhetspolicy

Antagen av kommunstyrelsen 1999-03-03 § 46-99

# IT-säkerhetspolicy

## Lysekils kommun

### IT-säkerhetspolicy för Lysekils kommun

Denna policy uttrycker kommunledningens syn på behovet av IT-säkerhet i Lysekils kommun. Den anger omfattning och ansvarsfördelning för hur IT-säkerhetsarbetet skall bedrivas.

#### **Definitioner**

Med Lysekils kommun avses samtliga kommunala förvaltningar. Beträffande skolans verksamhet kan vissa ytterligare anvisningar tillkomma.

Informationssäkerhet omfattar både traditionell datasäkerhet och säkerhet som hänför sig till hantering av information i olika verksamheter. Information är idag en viktig resurs för Lysekils kommun. Om inte informationen hanteras på rätt sätt kan stora skador uppstå.

Det är inte bara hemlig, känslig eller annars värdefull information som måste skyddas. Även öppen information måste skyddas mot t ex obehörig förändring dvs att informationen blir felaktig.

Begreppet IT-säkerhet används för skyddsåtgärder som är av teknisk karaktär (t ex olika former av behörighetskontrollsystem samt skydd av hård- och mjukvara).

#### **Kommentar**

Då detta är den första IT-säkerhetspolicyen kommer den att innehålla ett antal förslag till åtgärder som behöver genomföras inom IT-säkerhetsområdet. Dessa är samlade i slutet av detta dokument under rubriken ***"Förslag till åtgärder inom IT-säkerhetsområdet"***.

#### **Krav**

Den ökade användning av IT-system ställer ökade krav på dessa. Det ställs också allt högre krav på funktionalitet och säkerhet.

Olika intressenter ställer kraven på IT-säkerhet. Inom organisationen ställer både ledning och användare krav. Andra intressenter som ställer krav på IT-säkerhet kan vara medborgare och andra externa intressenter, t ex leverantörer.

# IT-säkerhetspolicy

## Lysekils kommun

Kraven på IT-säkerhet kan sammanfattas i fyra punkter:

- **Riktighet**

Producerad information skall vara korrekt, aktuell och begriplig.

- **Tillgänglighet**

IT-systemen skall vara tillgängliga för de behöriga användarna.

- **Sekretess**

Information och program skall skyddas så att de inte avsiktligt eller oavsiktligt görs tillgängliga eller avslöjas för obehöriga eller att de utnyttjas på ett felaktigt sätt.

- **Spårbarhet**

Det skall finnas funktioner och rutiner som gör det möjligt att härleda alla operationer i IT-systemet till enskilda individer och program.

### ***Motiv för IT-säkerhet***

Ett fungerande IT-stöd är en förutsättning för att kommunens verksamhet skall fungera och kunna bedrivas effektivt. Beroendet av IT-stöd är idag mycket stort och huvuddelen av verksamheten klarar sig inte utan detta utan allvarliga konsekvenser och störningar. Nya system tillkommer hela tiden, komplexiteten i dessa ökar och beroendet blir ständigt allt större.

Även mycket måttliga driftstörningar kan få betydande negativa konsekvenser både för den direkt berörda verksamheten och för andra verksamheter.

Större och mer omfattande driftstörningar kan få mycket negativa konsekvenser och kan bli ekonomiskt omfattande både för den egna verksamheten och för andra samhällsfunktioner. Vad händer t ex om utbetalning av socialbidrag inte kan ske eller om vi inte kan tillgodose kravet på offentlighet beroende på att det datasystem som hanterar diareföring inte fungerar.

För att minimera riskerna av att IT-verksamheten drabbas av allvarliga störningar måste en viss IT-säkerhetsnivå uppnås och upprätthållas.

### ***IT-säkerhetsnivå***

IT-säkerheten skall ha en nivå som överensstämmer med de övergripande målen för kommunens verksamhet. Detta innebär bland annat att hänsyn ska tas till:

# IT-säkerhetspolicy

## Lysekils kommun

- de övergripande säkerhetskrav som ställs på verksamheten ( t ex sekretessregler i socialtjänsten)
- lagar som direkt påverkar verksamheten
- den årliga skadekostnad som kan accepteras i olika IT-system och totalt för IT-verksamheten
- interna och externa intressenters krav på korrekt information
- personalens krav på en god social och fysisk arbetsmiljö

### **Organisation och ansvar**

#### Operativt ansvar

Ansvar för IT-säkerheten följer det operativa ansvaret på olika nivåer i kommunen. Detta innebär att:

- ledningen har det yttersta ansvaret för IT-säkerheten
- verksamhetsansvariga chefer har det operativa ansvaret för att de IT-system som verksamheten använder uppfyller kraven på IT-säkerhet

Det är emellertid värt att påpeka att det generella ansvaret för säkerhet även sträcker sig till den vanliga användaren av IT-system. Var och en som arbetar med IT-system har ett ansvar för att säkerheten inte eftersätts oavsett om arbetet regleras av säkerhetsregler eller inte.

#### Samordningsansvar

Ansvarig för samordning av IT-säkerhetsarbetet är **IT-samordnaren**. Denne har en rådgivande och samordnande funktion. I alla frågor som rör IT-säkerhet sker rapportering direkt till kommunledningen.

### **Riktlinjer för IT-säkerhetsarbetet.**

Dessa riktlinjer anger hur säkerhetsnivån skall uppnås upprätthållas inom Lysekils kommun.

#### Organisation och ansvar

# IT-säkerhetspolicy

## Lysekils kommun

Ansvaret för IT-säkerheten följer det operativa ansvaret. För varje verksamhetssystem (t ex ekonomisystem, personalsystem m fl) skall en systemägare fastställas. För ekonomisystemet är detta t ex ekonomichefen. Systemägaren utser en systemansvarig och en eller flera ersättare för denne. Systemägare, systemansvarig samt ersättare för varje verksamhetssystem skall finnas dokumenterade och finnas tillgängliga på IT-enheten samt på respektive förvaltning..

| System | Systemägare | Systemansvarig | Ersättare |
|--------|-------------|----------------|-----------|
|        |             |                |           |
|        |             |                |           |

Översyn av IT-säkerheten skall göras fortlöpande. Ansvaret för denna översyn vilar på den IT-säkerhetsansvarige. Vid behov skall en handlingsplan med förslag till åtgärder upprättas årligen. En gång per år skall en skriftlig redogörelse lämnas till kommunledningen om genomförda IT-säkerhetsåtgärder. Observera att denna vid behov kan behöva sekretessbeläggas.

### **Informationsklassning**

För att kunna ta ställning till vilka skyddsåtgärder som måste vidtas måste man klarlägga dels vilka de största riskerna för störningar är, dels vilka delar av verksamheten som är ömtåligast för störningar.

Informationsklassificering är en delprocess i arbetet med IT-säkerhet. Skälet till att informationen behöver skyddas kommer från olika krav:

- lagar, t ex datalagen, sekretesslagen
- säkerhetskrav, t ex föreskrifter från försvarsmakten eller myndigheter
- övriga krav, t ex ekonomiska krav inom företag eller medborgare som skall ha tillgång till information

En generell rekommendation är att **all** information klassificeras.

Verksamheten kan vara känslig för störningar på två sätt. Dels kan den information som produceras i IT-systemen vara så viktigt att om den faller bort eller förstörs, kan verksamheten inte bedrivas på normalt sätt under kortare eller längre tid. Dels kan informationen på ett eller annat sätt vara konfidentiell och kan vålla skada om den hamnar i fel händer.

Ansvaret för informationsklassning ligger på verksamhetsansvariga chefer. Sekretesslagstiftningens regler spelar också en roll här.

Exempel på klassificering av information.

# IT-säkerhetspolicy

## Lysekils kommun

### **Klass 1. Kritisk information**

Information som inte kan undvaras ens under en kort tid utan stora men för verksamheten.

### **Klass 2. Normal information**

Information som kan undvaras under en kortare period.

### **Klass 3. Perifer information.**

Information som kan undvaras under längre perioder.

Det skall finnas mätbara mål för informationens tillgänglighet.

### **Klassificering av information efter sekretess.**

Klassificeringen skall göras med utgångspunkt från sekretesslagen och offentlighetsprincipen.

#### **Klass 1. Information som klassificeras som hemlig eller kvalificerat hemlig med hänsyn till rikets säkerhet.**

Denna information får endast hanteras i system med mycket höga krav på behörighetskontrollsystem

#### **Klass 2. Övrig enligt sekretesslagen sekretessbelagd information.**

Här kan det röra sig om personuppgifter som bedöms känsliga ur integritetssynpunkt.

#### **Klass 3. Arbetsmaterial.**

Även denna typ av information kan behöva skyddas från insyn.

# IT-säkerhetspolicy

## Lysekils kommun

### **Klass 4. Offentlig information.**

Information som enligt offentlighetslagstiftningen är öppen för alla inom och utom organisationen.

(Statskontoret har givit ut en skrift som ger en bra handledning för arbetet med informationsklassning, *Handbok i IT-säkerhet 1997:29a-c*)

### **Fysiskt skydd**

Fysiskt skydd av IT-utrustning kan behövas av olika skäl. Man kan vilja skydda sig mot stöld och skadegörelse, brand, vatten, avbrott i elförsörjning med mera.

Tillträdesskydd är viktigt bland annat med tanke på att datorutrustning och olika datorkomponenter är stöldbegärliga.

Datorutrustning bör helst inte placeras i närheten av fönster i markplanet. Dessutom bör de inte placeras i lokaler dit allmänheten har tillträde utan att utrustningen kan övervakas.

Bärbara datorer är särskilt lätta att stjäla. Bärbara datorer får t ex aldrig lämnas obevakade i bilar eller på annan plats där de lätt kan stjälas. En särskild risk med bärbara datorer är att de ibland kan vara förkonfigurerade för åtkomst till kommunens nät vilket kan medföra att en bärbar dator i orätta händer kan ställa till stor skada.

Lokaler som innehåller datorutrustning bör vara utrustade med inbrottslarm. Vid behov kan datorer och skrivare förses med stöldskydd vilka finns i ett stort antal och utförande på marknaden.

Centrala servrar skall vara placerade i ett särskilt serverrum vilket skall vara låst. Rummet skall vara utrustat med brandlarm, inbrottslarm, larm för förhöjd temperatur samt larm för utströmmande vatten.

Datorutrustning (datorer, skrivare, bildskärmar) skall vara stöldmärkt och utrustningen skall finnas förtecknad i ett register som ständigt hålls uppdateras. Registret skall vara säkerhetskopierat och säkerhetskopieringen skall förvaras i låst och brandskyddat kassaskåp. Registret (inventarieförteckningen) skall innehålla uppgifter om serienummer, fabrikat, typ, leverantör, leveransdatum, garantitid och placering.

Det är särskilt viktigt att skydda de centrala serverna. Dels är informationen viktig att skydda, dels representerar utrustningen i sig ett stort värde.

Serverrummet skall inte användas till annan än övervakning, service o dyl. Ingen förvaring av brandfarligt material får förekomma i rummet. Rummet skall också städas regelbundet för att undvika damm så långt som möjligt då detta dels kan vara brandfarligt, dels kan det skada känsliga komponenter som hårddiskar.

Inga obehöriga får vistas i serverrummet utan övervakning. Detta gäller även servicetekniker. I anslutning till serverrummet skall finnas brandsläckare som är lämplig till att släcka bränder i elektronisk utrustning.

# IT-säkerhetspolicy

## Lysekils kommun

I serverrummet skall även finnas klimatanläggning som kan ge erforderlig låg temperatur. Om möjligt bör även reservutrustning för kyla finnas.

Vatten- och avloppsledningar bör inte passera genom serverrummet.

Serverrummet bör ha separat matning av elström (egen grupp) och det bör även finnas en central strömbrytare till serverrummet. Denna skall naturligtvis placeras på ett skyddat ställe så att den inte kan komma åt av obehöriga.

Serverrummet bör om möjligt ligga långt inne i byggnaden.

Det är emellertid inte bara hårdvaran som måste ha ett fysiskt skydd. Även media med originalprogramvara måste skyddas på ett tillräckligt sätt. Det kan röra sig om band, CD-skivor eller disketter med programvara. Dessa skall förvaras i brandskyddat kassaskåp på annan plats än i serverrummet. Kassaskåpet skall vara av brandskyddsklass A120. Skåpet skall vara låst när det inte används. Skåpet kan även användas till förvaring av säkerhetskopior.

### **Behörighetskontrollsystem (BKS)**

I Lysekils kommun krävs BKS dels för åtkomst till nätet med centrala resurser, dels BKS för åtkomst till verksamhetsspecifika applikationer. Krav på BKS för dessa ställs upp av respektive verksamhet.

För inloggning på nätet med dess centrala resurser krävs dels en användaridentitet, dels ett lösenord. Beställning av användaridentitet skall göras på särskild blankett (bifogas) underskiven av ansvarig chef. Blanketten förvaras på IT-enheten. Lösenordet skall bestå av minst fem tecken varav två skall vara siffror. Lösenordet måste bytas var 30:e dag och vid fler än tre misslyckade inloggningsförsök låses användaridentiteten. Om användaridentiteten inte använts på mer än 45 dagar spärras den. Det åligger också ansvariga chefer att meddela IT-enheten när en användaridentitet skall upphöra att gälla. Anmälan görs på ovan nämnda blankett.

Servicepersonal skall skriva under förbindelse om tystnadsplikt innan arbete påbörjas i kommunens datautrustning.

Behörighet till verksamhetsspecifika applikationer hanteras av respektive verksamhet som också ställer upp de behörighetskrav som skall gälla för dessa system. Tilldelning av användaridentiteter skall ske på samma sätt som till de gemensamma systemen.

Skärmläckare med lösenord skall användas på arbetsplatserna.

Obehöriga personer får inte använda kommunens datorutrustning.

### **Driftsäkerhet**

Det är av yttersta vikt för kommunens verksamhet att IT-systemen har så hög driftsäkerhet som möjligt. Driftavbrott är mycket kostsamma och måste undvikas så långt detta går. Ett antal åtgärder kan vidtas för att uppnå en hög driftsäkerhet.

# IT-säkerhetspolicy

## Lysekils kommun

### Kompetens (intern)

IT-personalen måste ha en hög kompetens för att snabbt kunna åtgärda fel. Om man är beroende av resurser utanför kommunens organisation blir ofta driftavbrotten längre med stora kostnader för stillestånd som följd.

### Kompetens (extern)

I vissa fall anlitas extern kompetens och det är då viktigt att man har klara avtal som bland annat klargör vilka inställelsetider som gäller. Det är också viktigt att man ser över vilka garantibestämmelser som gäller för IT-utrustningen.

### Säkerhetskopiering

En av de viktigaste åtgärderna för att skapa en säker driftmiljö är att ha väl fungerande rutiner för säkerhetskopiering.

De centrala servrarna säkerhetskopieras varje natt (måndag-fredag). Hela innehållet på servrarna kopieras. Fyra generationer band skall finnas, dessutom skall en månadskopia tas sista fredagen varje månad. Denna förvaras för sig. All säkerhetskopiering dokumenteras i driftlogg.

Beträffande verksamhetssystem fastställer systemägare/systemansvarig med vilken periodicitet säkerhetskopiering skall göras. Säkerhetskopieringen görs för närvarande av IT-personalen och säkerhetskopiorna förvaras i säkerhetsskåp.

Vid uppgradering av systemprogramvaran skall alltid en säkerhetskopia tas innan arbetet påbörjas. Denna kopia förvaras i tillräckligt lång tid. När det gäller vissa verksamhetssystem, t ex ekonomisystemet, finns särskilda regler för hur säkerhetskopior på gamla systemversioner skall förvaras.

Band som används till säkerhetskopiering har en begränsad livslängd och måste bytas med jämna mellanrum. Hur lång tid som skall gå mellan bandbyten avgörs bland annat av hur ofta banden används.

En gång i månaden skall prov med återläsning av information från banden göras för att säkerställa att informationen på dessa är tillgänglig och läsbar. Ansvaret för detta ligger på IT-enheten när det gäller de centrala systemen och på respektive verksamhet beträffande de verksamhetsspecifika systemen.

All säkerhetskopiering, prov med återläsning samt alla driftstörningar skall dokumenteras i en driftlogg som förvaras i serverrummet. Även systemuppgraderingar, versionsbyten m m skall dokumenteras i denna.

### **Dokumentation**

# IT-säkerhetspolicy

## Lysekils kommun

För att säkerställa driften måste systemen finnas dokumenterade på ett tillfredsställande sätt. Denna dokumentation skall också avse datakommunikationens infrastruktur samt fastighetsnätet både i kommunhuset och andra byggnader där fastighetsnät finns installerade. En god dokumentation är ett effektivt sätt att gardera sig mot alltför stort beroende av nyckelpersoner. Varje systemförändring skall dokumenteras av respektive leverantör. Dessa skall också avkrävas dokumentation vid installationer. Vid behov skall detta skrivas in i kravspecifikationen vid upphandlingar av nya system.

Dokumentationen skall förvaras i säkerhetsskåp och skall även vid behov sekretessbeläggas.

### **Planer för reservdrift**

Eftersom det inte är ekonomiskt möjligt eller rimligt att gardera sig för alla de störningar som kan drabba ett IT-system kan det i vissa fall vara befogat att ha någon plan för reservdrift vid längre driftavbrott.

Behovet av reservdrift får bedömas utifrån den risk- och sårbarhetsanalys man genomfört. Ett alternativ till reservdrift kan vara manuella rutiner. Inte minst med tanke på de eventuella störningar som kan tänkas uppkomma i samband med millennieskiftet kan det vara befogat att se över vilka manuella reservrutiner som det kan vara befogat att aktualisera (t ex manuell utbetalning av socialbidrag).

I detta sammanhang kan man också poängtera behovet av att ha tillgång till reservkraft för att kunna driva datasystem och datakommunikation samt fastighetsnät även vid ett längre bortfall av elförsörjningen

Man kan också tänka sig att planera reservdrift i samarbete med närliggande kommuner. Det kan gå till så att var och en av de aktuella kommunerna reserverar utrymme i servrar och på hårddiskar. En absolut förutsättning för att detta skall fungera är att man använder samma operativsystem, samma version av operativsystem med mera. En sådan överenskommelse måste regleras i avtal mellan de inblandade kommunerna.

Man kan även tänka sig att upprätta avtal med leverantör eller servicebyrå för att klara av reservdrift. Detta torde dock bli en kostsam lösning som dock måste bedömas utifrån risk- och sårbarhetsanalysen.

Det måste också finnas klart dokumenterat vid vilka lägen man går över till reservdrift. Observera att denna planering för reservdrift inte avser läget vid beredskap eller krig.

### **Avbrottsplan**

Även detta är ett område som bör ses över inför millennieskiftet med de risker det kan medföra i datadriften.

*En avbrottsplan skall beskriva de förberedda åtgärder som ska vidtas när ett avbrott i IT-stödet inträffar. Planeringen skall täcka olika situationer, från ett kort avbrott med lindriga konsekvenser till ett längre avbrott med allvarliga konsekvenser.*

# IT-säkerhetspolicy

## Lysekils kommun

Avbrottsplanen skall beskriva åtgärder som:

- minskar skadorna vid ett oförutsett driftavbrott
- vid behov och om det är möjligt, ersätter det IT-stöd som användarna är beroende av
- hur information lämnas om avbrottet till berörda såväl inom som utom organisationen

Informationen i avbrottsplanen bör hållas tillgänglig för så få personer som möjligt.

### Förslag till åtgärder inom IT-säkerhetsområdet

| Åtgärd  | Utförs av                   | Ansvarig | Klar senast |
|---|-----------------------------|----------|-------------|
| Informationsklassning                         | Resp förvaltning            |          |             |
| Sårbarhetsanalys på nyckelpersoner            | Resp förvaltning            |          |             |
| Katastrofplanering                            | LKS                         |          |             |
| Inventering av centrala system                | IT-enheten                  |          |             |
| Inventering av verksamhetssystem              | Resp verksamhet             |          |             |
| Fastställande av systemägare                  | IT-enheten, resp verksamhet |          |             |
| Fastställande av systemansvarig och ersättare | IT-enheten, resp verksamhet |          |             |
| Dokumentera centrala system                   | IT-enheten                  |          |             |

# IT-säkerhetspolicy

## Lysekils kommun

|                               |                             |  |  |
|-------------------------------|-----------------------------|--|--|
| Dokumentera verksamhetssystem | Resp verksamhet             |  |  |
| Dokumentera infrastruktur     | IT-enheten                  |  |  |
| Genomföra sårbarhetsanalys    | LKS                         |  |  |
| Planering av reservdrift      | IT-enheten                  |  |  |
| Upprätta avbrottsplan         | IT-enheten, resp verksamhet |  |  |