UTGÅVA 3

# Basnivå för informationssäkerhet (BITS)

KBM REKOMMENDERAR ▪ 2006:1

KRISBEREDSKAPS
MYNDIGHETEN

KBM REKOMMENDERAR ■ 2006:1

# Basnivå för informationssäkerhet (BITS)

Titel: Basnivå för informationssäkerhet (BITS)
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Ablestock
Upplaga: 15 000 exemplar

ISSN: 1652-2893
ISBN: 91-85053-97-x
KBM:s dnr 1214/2005
Grafisk form: AB Typoform
Tryck: Edita, Västerås 2006

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

KBM REKOMMENDERAR 2006:1

# Innehåll

# Förord

Det finns ett behov av att arbeta på ett strukturerat och enhetligt sätt när det gäller att uppnå och upprätthålla önskvärd nivå för informationssäkerheten. Ett antal olika standarder och standardiseringssträvanden förekommer på olika håll, både nationellt och internationellt. Ett utökat informationsutbyte har också medfört ett ökat behov av internationellt överenskomna standarder.

De internationella organisationerna International Organization for Standardization (ISO) och International Electrotechnical Commission (IEC) utgör tillsammans ett system för internationell standardisering. Inom ramen för detta har standarder godkänts som också blivit svenska standarder. Den svenska benämningen för dessa är SS-ISO/IEC 17799 respektive SS 627799-2.

Inom ramen för arbetet med "24-timmarsmyndigheten" har Statskontoret tagit fram produkten OffLIS som utgör riktlinjer för arbetet med att uppfylla dessa standarder.

Viktiga moment i revideringen av skriften Basnivå för IT-säkerhet (BITS) har varit att få den att till sin struktur överensstämma med de svenska standarderna och att även involvera väsentliga delar av OffLIS. Ambitionen är därmed att underlätta det mer långsiktiga arbetet med att uppfylla de svenska standarderna och att även kunna ersätta OffLIS.

*Ann-Louise Eksborg*
Generaldirektör, Krisberedskapsmyndigheten

# 1. Omfattning

## 1.1 BITS tillämplighet

I denna skrift, BITS (Basnivå för informationssäkerhet), redovisas ett antal rekommenderade administrativa säkerhetsåtgärder som minst bör vidtas för att uppnå en acceptabel säkerhetsnivå för informationshanteringen i en organisation. Denna säkerhetsnivå betecknas *basnivå*. I första hand riktas dessa rekommendationer mot den informationshantering inom samhällsviktig verksamhet som måste kunna fungera även under olika grader av störningar i samhället. Ambitionen är att basnivån ska vara väl balanserad och ge en generellt acceptabel säkerhetsnivå. Om basnivån är tillräcklig för den enskilda organisationen kan dock endast avgöras genom en riskanalys.

## 1.2 Ändringar i förhållande till tidigare version

I relation till förra utgåvan av BITS har följande revideringar vidtagits:

- Betydelsen av förkortningen BITS har ändrats från "basnivå för IT-säkerhet" till "basnivå för informationssäkerhet". Förkortningen BITS bibehålls dock eftersom den är väl inarbetad.
- Kapitel- och avsnittsindelningen följer nu den svenska standarden SS-ISO/IEC 17799.
- Innehållet har utökats till att omfatta hela begreppet informationssäkerhet.
- Det huvudsakliga innehållet i Statskontorets mallregelverk OffLIS är inarbetat i BITS och BITS kommer därför att ersätta detta. Skriften BITS kan, på samma sätt som OffLIS, användas som mall för att upprätta ett regelverk för informationssäkerhetsarbetet i enlighet med svenska standarden SS-ISO/IEC 17799.

# 2. Termer och definitioner

Används skriften BITS som mall för en organisations regelverk för informationssäkerhetsarbetet föreslås följande redovisas under detta avsnitt:

- Termer och definitioner av värde för organisationen.
- Uttalande om vilka delar i svenska standarden SS-ISO/IEC 17799 som är tillämpliga för organisationens behov. Ett formellt sådant är ett krav vid certifiering av en verksamhet mot standarden.

Följande begrepp är av central betydelse i BITS.

**Informationssäkerhet:** Förmågan att upprätthålla önskad sekretess (konfidentialitet), riktighet och tillgänglighet avseende information och informationstillgångar.

**Systemägare:** Organisationens chef eller av denne särskilt utsedd aktör med ansvar för anskaffning, ny-/vidare-/avveckling, förvaltning samt ansvar för krav på drift, säkerhet och användning av ett informationssystem inom ramen för antagna mål och ekonomiska ramar.

**Central systemägare:** Systemägare vid en organisation som har det övergripande ansvaret för ett informationssystem som används inom flera organisationer.

**Informationssäkerhetssamordnare/-funktion:** En eller en grupp av personer som är den sammanhållande länken mellan den operativa verksamheten för informationsäkerhet och ledningen.

**Informationssäkerhetspolicy:** Dokument som anger mål och inriktning för organisationens informationssäkerhetsarbete.

**Systemsäkerhetsanalys*:** Dokument avseende ett enskilt informationssystem eller internt IT-nätverk som redovisar de samlade kraven på detta avseende tillgänglighet, riktighet och sekretess (konfidentialitet). Av säkerhetsanalysen ska framgå vilka säkerhetsåtgärder som är vidtagna samt de eventuella ytterligare säkerhetsåtgärder som behöver vidtas för att kraven på informationssystemet ska uppfyllas. Säkerhetsanalysen ska vara avstämd mot organisationens informationssäkerhetspolicy.

**Säkerhetsinstruktion:** Konkreta regler och rutiner avseende informationssäkerhet som riktar sig till användare, driftpersonal och personal för administration och förvaltning.

**Basnivå:** Säkerhetsnivå som minst måste uppnås för ett informationssystem som bedöms nödvändigt för att upprätthålla en verksamhet på en acceptabel nivå.

**Driftgodkännande:** Formellt organisationsbeslut att godkänna ett informationssystem för drift.

* Ersätter det tidigare begreppet "systemsäkerhetsplan".

# 3. BITS STRUKTUR

## 3.1 Innehåll

BITS är upplagt enligt följande:

- Kapitel- och avsnittsindelningen följer den svenska standarden SS-ISO/IEC17799
- Varje avsnitt inleds med citat av de mål som formuleras under motsvarande avsnitt i SS-ISO/IEC17799
- Efter dessa målformuleringar redovisas ett antal rekommendationer för basnivå.
- Den efterföljande texten redovisar, i olika utsträckning, viss kompletterande information till redovisade rekommendationer.

## 3.2 Säkerhetsarbetets olika steg

BITS utgår från följande arbetsprocess för informationssäkerhetsarbetet:

- Organisationen definierar målen och inriktningen för säkerhetsarbetet i en informationssäkerhetspolicy. Denna är det övergripande dokument som styr informationssäkerhetsarbetet.
- Informationssäkerhetspolicyn konkretiseras i säkerhetsinstruktioner för användare, för kontinuitet och drift samt för personal för administration och förvaltning. I vissa fall kan det även finnas behov av systemspecifika instruktioner.
- Utgående från informationssäkerhetspolicyn görs en systemsäkerhetsanalys för varje informationssystem som bedöms viktigt för verksamheten. Systemsäkerhetsanalysen beskriver vilka säkerhetskrav som ska ställas utifrån aspekterna sekretess, riktighet och tillgänglighet. Om kraven överstiger den basnivå som definieras i KBM:s rekommendationer behövs kompletterande säkerhetsåtgärder.

- En bedömning av om genomförda säkerhetsåtgärder har avsedd funktion samt ett ställningstagande till hur ytterligare krav på säkerhetsåtgärder ska hanteras ger underlag för den säkerhetsutvärdering som ett beslut om driftgodkännande ska baseras på.

# 4. Riskbedömning och riskhantering

## 4.1 Utgångspunkt för informationssäkerhetsarbetet

Utgångspunkten för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klarlägga den säkerhetsnivå som ska gälla för skydd av en organisations information och informationssystem. Den basnivå som föreslås i BITS kan endast ses som en lägsta nivå som inte bör underskridas.

## 4.2 KBM:s verktyg för analys av informationssäkerhet

En riskanalys behöver genomföras för att klarlägga om det krävs en högre nivå av säkerhet än den som KBM:s basnivå definierar. KBM har tagit fram ett verktyg för att göra en sådan analys (BITS Plus*). I verktyget definieras ytterligare två säkerhetsnivåer utöver BITS:s basnivå. I korthet omfattas verktyget av följande moment:

- Aktuellt informationssystem beskrivs avseende avgränsning, kommunikation och informationsinnehåll
- Kraven på tillgänglighet, riktighet och sekretess (konfidentialitet) klarläggs
- Verktyget
  - genererar administrativa åtgärdsförslag som svarar mot ställda krav
  - skapar dokumentet systemriskanalys
  - skapar resultatrapporter
- Mallar för dokument som styr informationssäkerhetsarbetet redovisas

* Vidareutveckling av KBM:s IT-säkerhetsguide.

# 5. Säkerhetspolicy

## 5.1 Informationssäkerhetspolicy

**Mål:** "Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med organisationens verksamhetskrav och relevanta lagar och föreskrifter."

### Basnivå

- Det ska finnas en av ledningen fastställd informationssäkerhetspolicy
- Policyn ska uttrycka
  - ledningens engagemang
  - definition, omfattning och vikten av informationssäkerhet
  - mål och metoder för styrning
  - struktur för riskbedömning och riskhantering
- Informationssäkerhetspolicyn ska minst omfatta en kort beskrivning av
  - långsiktiga mål för informationssäkerheten
  - organisation, roller och ansvar för informationssäkerhetsarbetet
  - generella krav för utpekade områden av särskild betydelse för organisationen
- Ledningen ansvarar för att informationssäkerhetspolicyn
  - är dokumenterad
  - all personal får information om innehållet i denna och övriga regelverk
  - granskas med planerade intervall eller som en följd av betydande ändringar

Informationssäkerhetsarbetet utförs oftast av säkerhetsorganisationen men ledningen måste vara nära involverad eftersom det är deras viljeinriktning som ska speglas.

Policyn ska vara kortfattad och tydlig så att all personal ska kunna ta den till sig och så att den blir ett riktmärke i det fortsatta arbetet.

Policyn ska vara övergripande, relativt långsiktig för att inte behöva uppdateras alltför ofta.

**Tips**!
Se exempel på mall för informationssäkerhetspolicy på KBM:s hemsida (www.krisberedskapsmyndigheten.se).

# 6. Organisation av informationssäkerheten

## 6.1 Intern organisation

**Mål:** "Att hantera informationssäkerhet inom organisationen."

### Basnivå

- Ledningen ska
  - tillgodose behovet av resurser för informationssäkerhet
  - besluta hur informationssäkerhetsarbetet ska bedrivas i form av mål, organisation, ansvar och roller
  - säkerställa att åtgärder för informationssäkerhet som införs samordnas i hela organisationen
  - identifiera eventuellt behov av intern eller extern specialistrådgivning
  - godkänna metoder för riskbedömning, informationsklassning och godkännande
  - identifiera viktiga ändringar av den övergripande hotbilden
  - initiera en oberoende granskning av organisationens metod för att hantera informationssäkerheten och dess tillämpning
- Det ska finnas av ledningen beslutade informationssäkerhetsinstruktioner för förvaltning, för användare samt för kontinuitet och drift
- Det ska finnas en informationssäkerhetssamordnare/-funktion för informationssäkerhet
- Informationssäkerhetssamordnaren/-funktionen ska i frågor om informationssäkerhet vara direkt underställd organisationens chef
- Samtliga informationssystem ska vara identifierade och förtecknade samt godkända av ledningen.
- Av systemförteckningen ska framgå vilka system som är viktiga för verksamheten även vid störningar och kriser

- Samtliga informationssystem ska uppfylla basnivån enligt BITS
- Systemägare för samtliga informationssystem ska vara utsedda av ledningen
- Systemägare är ansvariga för att systemsäkerhetsanalys upprättas för de egna viktiga systemen
- Ledningen ska besluta om vilken risknivå som kan godtas
- All information ska klassas avseende sekretess (konfidentialitet), riktighet och tillgänglighet
- Det ska finnas en gemensam kontinuitetsplan för organisationen
- Nödvändiga avtal inom informationssäkerhetsområdet ska upprättas

För vissa områden inom organisationens verksamhet kan det finnas anledning att ta fram speciella regler, exempelvis vad som ska gälla för distansarbete och användning av Internet.

Ledningen har alltid det övergripande ansvaret för verksamheten och de informationssystem som används som stöd. Delegering av ansvaret för informationssäkerhet sker normalt enligt samma principer som gäller för delegering av verksamhetsansvaret i övrigt inom organisationen.

Detaljer som berör enskilda informationssystem redovisas i de systemsäkerhetsanalyser som ska finnas för respektive informationssystem. Systemsäkerhetsanalyser kan behöva revideras vid exempelvis förändringar i verksamhetens inriktning och omfattning, större ändringar i systemens utformning, förändringar i hotbilden o.dyl.

Den rådgivande och samordnande funktionen bör bl.a. ha som uppgift att:

- samordna informationssäkerhetsarbetet inom organisationen
- medverka i framtagning av informationssäkerhetspolicy, övriga styrdokument, systemsäkerhetsanalyser och säkerhetsinstruktioner
- informera om och ge råd i informationssäkerhetsfrågor
- medverka i genomförandet av säkerhetsåtgärder
- följa upp att säkerhetsinstruktioner följs och vid behov föreslå åtgärder

- samordna och delta i framtagningen av generella rutiner avseende informationssäkerheten inom organisationen, exempelvis när det gäller rutiner för incidenthantering.
- svara för omvärldskontakter/omvärldsbevakning
- samordna resurser och information för hantering av säkerhetsincidenter

**Tips!**
Använd KBM:s analysverktyg (BITS Plus) för att upprätta systemsäkerhetsanalyser.

Exempel på mallar för informationssäkerhetsinstruktioner finns på KBM:s hemsida (www.krisberedskapsmyndigheten.se).

Vid upprättande av systemförteckning kan BITS Plus användas.

## 6.2 Utomstående parter

**Mål:** "Att bibehålla säkerheten hos organisationens information och resurser för informationsbehandling som är åtkomlig, bearbetas, kommuniceras till eller styrs av utomstående parter."

**Basnivå**

- Det ska finnas dokumenterade regler för tredjeparts åtkomst till information eller informationssystem
- Extern personal (servicepersonal, konsulter, hantverkare) ska informeras om reglerna för åtkomst, tillträde, brandskydd etc.
- Riskanalys ska föregå beslut om utläggning (outsourcing) av informationshantering eller informationssystem.

Om organisationen lägger ut informationsbehandling på en utomstående organisation bör ansvaret för informationssäkerheten regleras i avtal. Avtalet bör bl.a. beakta följande:

- hur de rättsliga kraven ska uppfyllas, både affärs- och säkerhetsmässigt, till exempel rörande lagstiftning om personuppgifter
- vilka åtgärder som ska vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar
- hur riktighet och sekretess rörande organisationens verksamhetstillgångar kan upprätthållas och testas
- vilka fysiska och logiska åtgärder som kommer att vidtas för att begränsa åtkomsten till organisationens känsliga information till enbart behöriga användare
- hur verksamheten kommer att kunna hållas igång vid en eventuell katastrofhändelse
- vilken fysisk säkerhetsnivå som ska gälla för utrustning som läggs ut
- revisionsrättigheter – det bör säkerställas att organisationen har rätt att genomföra revision av säkerheten hos tjänsteleverantören.
- om utläggning omfattar information som rör rikets säkerhet ska SUA-avtal tecknas, d.v.s. säkerhetsskyddad upphandling med säkerhetsskyddsavtal.

# 7. Hantering av tillgångar

## 7.1 Ansvar för tillgångar

**Mål:** "Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar."

**Basnivå**

- Informationsbehandlingsresurser ska vara förtecknade och märkta enligt gällande anvisningar (Säkerhetsinstruktion, förvaltning)
- Det ska finnas en ansvarsfördelning för organisationens samtliga informationstillgångar (Säkerhetsinstruktion, förvaltning).
- Omflyttning och överlåtelse av IT-utrustning till annan användare ska ske enligt fastställda rutiner (Säkerhetsinstruktion, förvaltning och Säkerhetsinstruktion, kontinuitet och drift).
- Regler för hur informationsbehandlingsresurser får användas ska dokumenteras (Säkerhetsinstruktion, förvaltning).

Exempel på tillgångar som hör till informationssystem är:

- Informationstillgångar: Databaser och datafiler, systemdokumentation, användaranvisningar/-manualer, utbildningsmaterial, administrativa rutiner, drift- och servicerutiner, kontinuitetsplaner, avbrottsplaner, arkiverad information
- Programtillgångar: Tillämpningsprogram, nätverk- och operativsystemprogram, utvecklingsverktyg
- Fysiska tillgångar: Datorutrustning (datorer, bildskärmar), kommunikationsutrustning (modem, hubbar, routrar, telefonväxlar, faxmaskiner, telefonsvarare, telefoner, mobiltelefoner), lagringsmedia (band och skivor), annan teknisk utrustning (reservaggregat, klimatutrustning)

## 7.2 Klassificering av information

**Mål:** "Att säkerställa att informationstillgångar får en lämplig skyddsnivå."

**Basnivå**

- Det ska finnas dokumenterade regler för klassning av information (Säkerhetsinstruktion, användare).
- Information som behandlas i informationssystem ska klassificeras med hänsyn till krav på skyddsnivå.
- Systemägaren ansvarar för att klassificering görs och att säkerhetskraven tillgodoses.
- Det ska finnas regler för datamedia (Säkerhetsinstruktion, kontinuitet och drift) som omfattar:
  - klassning av datamedia
  - hur datamedia ska märkas och förtecknas

Om det ställs extrema krav på viss information i ett informationssystem, kan det övervägas om inte denna information ska tas bort ur systemet och behandlas i särskild ordning eller hanteras i en kompletterande procedur. På så vis kan ofta kraven på systemet sänkas.

På lagringsmedia kan information av olika klassningsgrad förekomma. Det är därför viktigt att även datamedia omfattas av klassning. Märkning och förteckning av datamedia bör gälla alla datamedier som hanteras inom organisationen, såväl användarnas som driftorganisationens. Avsikten med märkning och förteckning är att datamedia inte ska förväxlas. Även säkerhetskopior bör märkas och förtecknas.

För att inte riskera att klassificering görs slentrianmässigt, bör utbildning i hur detta ska ske genomföras med viss regelbundenhet, exempelvis vartannat år. Nyanställda bör få utbildning i gällande regler för informationsklassning innan de ges behörighet till informationssystem.

För offentlig förvaltning gäller att ett beslut om att lämna ut information som omfattas av sekretess alltid ska föregås av en sekretessprövning.

**Tips!**
Se klassningsmodellen i KBM:s analysverktyg (BITS Plus).

# 8. Personalresurser och säkerhet

## 8.1 Före anställning

**Mål:** "Att säkerställa att anställda, leverantörer och utomstående användare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser."

### Basnivå

- Vid anställning ska kontroll av bakgrund göras i proportion till kommande arbetsuppgifter
- Chefer i linjeorganisationen ansvarar för att medarbetare och inhyrd/inlånad personal får information om informations-säkerhetspolicy och -instruktioner
- Systemägaren ska definiera vilka krav som ska ställas på användare som ska få tillgång till informationssystemet och dess information och kraven ska
  - vara dokumenterade och kommunicerade
  - avse såväl säkerhet som kompetens.

## 8.2 Under anställningen

**Mål:** "Att säkerställa att anställda, leverantörer och utomstående användare är medvetna om hot och problem som rör informationssäkerhet, sitt ansvar och sina skyldigheter samt är utrustade för att stödja organisationens säkerhetspolicy när de utför sitt normala arbete och att minska risken för mänskliga fel."

**Basnivå**

- Det ska finnas dokumenterade, av ledningen beslutade, säkerhetsinstruktioner för användare (Säkerhetsinstruktion, användare)
- Utbildningsinsatser inom informationssäkerhet ska genomföras regelbundet.
- Det ska finnas användarhandledning för ett informationssystem.

Säkerhetsinstruktion för användare redovisar de generella informationssäkerhetsregler som gäller för personalens hantering av organisationens informationssystem och IT-resurser. Den kan exempelvis klargöra vad som gäller för framtagning, bearbetning, klassning och sparande av dokument, för den egna arbetsstationen, restriktioner för elektronisk post och användning av Internet m.m.

Det är viktigt att genomföra utbildningar kontinuerligt, både för att kunskapen om informationssäkerhet ska vara tillräcklig, men även för att bibehålla säkerhetsmedvetandet och motivationen för att upprätthålla säkerheten.

För den personal det berör bör speciell information ges om vad som följer de olika ansvarsrollerna som definieras i informationssäkerhetspolicyn.

Användarhandledningen för ett system utformas med hänsyn till användarens kunskaper och behov och kan utgöras av:

- manual som riktas till normalanvändaren
- grundläggande användarguide som riktas till nybörjare. Kan eventuellt vara av lathundskaraktär.

Användarhandledningen bör minst omfatta:

- övergripande beskrivning
- handhavande av systemets funktioner.
- systemets förvaltningsorganisation
- vart man vänder sig för att få hjälp samt med fel, förslag och incidentrapporter.
- säkerhetsbestämmelser för systemet och dess information.
- eventuella rutiner för utlämning av information

**Tips!**
Se exempel på mall för säkerhetsinstruktion, användare på KBM:s hemsida (www.krisberedskapsmyndigheten.se).

## 8.3 Avslutande av anställning eller förflyttning

**Mål:** "Att säkerställa att anställda, leverantörer och utomstående användare lämnar organisationen eller ändrar anställningsförhållande på ett ordnat sätt."

**BASNIVÅ**

- För anställda, leverantörer och utomstående användare ska gälla att
  - alla organisationens tillgångar som de förfogar över återlämnas
  - åtkomsträtten till information och informationsbehandlingsresurser ska dras in vid avslutat engagemang

# 9. Fysisk och miljörelaterad säkerhet

## 9.1 Säkrade utrymmen

**Mål:** "Att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information."

**Basnivå**

- Beslut om vem som ska få tillträde till datorrum för att kunna utföra sina arbetsuppgifter ska fattas med hänsyn till informationens skyddsbehov.
- För utrymmen med känslig information eller för informationssystems drift viktig dator- och kommunikationsutrustning ska:
  - tillträde regleras (Säkerhetsinstruktion, förvaltning)
  - tillträde registreras och dessa uppgifter förvaras säkert
  - obemannade utrymmen låsas
  - servicepersonal, städpersonal m.fl., under övervakning, ges tillträde endast när detta krävs.

Tillträde till utrymmen med för informationssystems drift viktig dator- och kommunikationsutrustning kan exempelvis ske manuellt eller med kontrollsystem där in- och utpasseringar loggas.

Skrivare, telefax, kopiator, skanner eller liknande utrustning som användas för sekretessbelagd eller i övrigt känslig information ska placeras i utrymmen som endast behörig personal har tillträde till.

Om, som komplement till åtgärder för tillträdesskydd, stöldskydd i form av fastlåsning av utrustning används, rekommenderas att låsanordning som uppfyller Stöldskyddsföreningens normer väljs.

För tillträdesskydd bör även bl.a. följande övervägas:

- tjänstekort/besöksbricka ska bäras synligt.
- tillträdesrättigheter beviljas och underhålls enligt särskild rutin

Om obehörig påträffas ska detta rapporteras som en säkerhetsincident.

## 9.2 Skydd av utrustning

**Mål:** "Att förhindra förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i organisationens verksamhet."

### Basnivå

- IT-utrustning som kräver avbrottsfri kraft ska identifieras och förses med sådan.
- Utrustning för avbrottsfri kraft ska testas regelbundet enligt leverantörens anvisningar.
- Elförsörjningen till centralt driftställe ska ske via en separat gruppcentral.
- I direkt anslutning till för driften viktig dator- och kommunikationsutrustning ska det finnas kolsyresläckare i erforderligt antal.
- Larm ska finnas för
  - brand
  - temperatur
  - fukt
- Larm ska:
  - vara kopplade till larmmottagare
  - testas regelbundet
- Brandbesiktning av datordriftställe ska genomföras i samråd med brandförsvaret.
- För datordriftställe ska gälla att
  - det ska placeras i brandsektionerat område
  - alla väggenomföringar ska vara brandtätade
  - utrymmet ska vara fritt från brännbart onödigt materiel.
- Det ska finnas möjlighet att reglera och mäta temperatur och fuktighet.
- Rutiner ska finnas för att spåra om datamedia med känslig information har bortförts från de lokaler de normalt förvaras i.

Utrustningar som kan behöva förses med avbrottsfri kraft kan vara vissa viktiga servrar, som exempelvis nätverksservrar, samt viss kommunikationsutrustning. Generellt är det tillräckligt om centrala servrar och datakommunikationsutrustningar skyddas mot ett elbortfall på cirka ett par timmar.

Vid brandlarm måste säkerställas att brandförsvaret ges möjligheter till snabbt tillträde. Helst bör utrymme med för driften viktig dator- och kommunikationsutrustning vara utrustad med automatisk släckningsanordning.

För kabeldragningar kan det vara aktuellt att skilja starkströms- och telekablar från varandra för att undvika interferens. För känsliga eller kritiska system kan också övervägas att initiera avsökning efter obehörig utrustning som anslutits till kablarna.

Om utrustning med känslig information ska tas ur bruk eller återanvändas ska informationen raderas på ett säkert sätt. Reservutrustning, ny utrustning som inte hunnit installeras och utrustning som ska återanvändas eller tas ur bruk ska förvaras i låsta utrymmen. För all datorutrustning/datamedia som skrotas kan övervägas om ett formellt skrotningsprotokoll bör upprättas.

På grund av stöldrisken bör särskild uppmärksamhet ägnas förvaring av utrustning för arbete utanför ordinarie arbetsplats. Beroende på vilken information utrustningen (PC inklusive tillbehör såsom extraminnen, USB-minnen, DVD, CD etc.) innehåller kan särskilda säkerhetsåtgärder behöva implementeras. Samma krav på nivå för säkerhetsskyddet som krävs för arbetsplats inom organisationen ska anordnas innan arbetsplatsen kan tas i bruk.

Underhållsavtal som har betydelse för systemet bör ägnas särskild uppmärksamhet.

Information och utrustning för informationsbehandling får inte föras ut från organisationens lokaler utan medgivande av ansvarig chef. Rutiner för utförsel som omfattar kvittering bör tas fram där detta är motiverat.

# 10. Styrning av kommunikation och drift

## 10.1 Driftrutiner och driftansvar

**Mål:** "Att säkerställa korrekt och säker drift av informationsbehandlingsutrustning."

### Basnivå

- Det ska finnas dokumenterade, av ledningen beslutade, säkerhetsinstruktioner för drift (Säkerhetsinstruktion, kontinuitet och drift)
- Det ska finnas driftdokumentation för ett informationssystem som minst omfattar
  - säkerhetskopiering
  - återstarts- och återställningsrutiner
  - hantering av revisionsspår och logginformation
- För driftdokumentation ska gälla att
  - den ska innehålla instruktioner om hur informationssystem ska installeras och konfigureras.
  - kopia av driftdokumentationen ska förvaras skyddad och åtskild från driftstället.
- Driftdokumentation ska inkludera regler för
  - identifiering och registrering av viktiga ändringar
  - planering och test av ändringar
  - rutin för formellt godkännande av föreslagna ändringar
- All driftdokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i informationssystem.
- Systemägaren fattar, i samråd med IT-ansvarig, beslut om tidpunkt för installation av nya programversioner.
- För drift av informationssystem ska finnas en fastställd plan för:
  - bemanning

- kompetenskrav
- ersättare för systemadministratör.

- Installation av nya programversioner ska dokumenteras.
- Det ska finnas dokumenterade rutiner för installationer av funktioner i nätet (Säkerhetsinstruktion, kontinuitet och drift).
- Det ska finnas rutiner för hantering av säkerhetsincidenter och funktionsfel (Säkerhetsinstruktion, kontinuitet och drift)
- System-/programutveckling och tester av modifierade system ska ske åtskilt från driftmiljön.
- Olika behörigheter ska användas för drift- och utvecklingsmiljö.
- Unika identiteter ska användas för personer som ges behörighet för tester och utveckling.
- Implementation av programvara i såväl drift- som utvecklingsmiljö ska ske av behörig personal.
- Regler ska finnas för delegering av:
  - resurser och ansvar för drift under olika driftbetingelser.
  - resurser för incidentberedskap och ledning/åtgärder vid inträffad incident.

Säkerhetsinstruktion för kontinuitet och drift avser den löpande hanteringen av driften, instruktioner för hur avbrott av olika längd ska hanteras, eventuella prioriteringar vid exceptionella händelser, hantering och förvaring av datamedia o.dyl.

Driftdokumentation är till för den personal som ansvarar för den dagliga driften av ett informationssystem och kan t.ex. omfatta:

- en översikt som visar informationssystemets plats i organisationens totala datadrift samt ingående utrustning
- det fysiska nätets struktur och ingående komponenter
- det logiska nätets struktur
- driftsinstruktioner för alla aktiviteter i driften
- konfigurationen, inställningar av olika parametrar i informationssystemet som t.ex. förändringar av default-inställningar i operativsystem,
- routingtabeller
- telefonnummer till leverantörer eller motsvarande.
- regler för styrning av ändringar i drift

Om verksamheten kräver en kontinuerlig drift av informationssystemet måste åtgärder vidtas för att kunna hantera situationer med begränsad personalstyrka. Grunden för att säkerställa driftsäkerheten är att organisation och ansvar för den ordinarie driften av informationssystemet är tydligt, att dokumentation är tillgänglig samt att driftpersonal har rätt utbildning. Att ansvaret för olika kontroller och uppföljningsmoment är fördelat är också väsentligt, liksom åtgärder för att upptäcka och korrigera fel.

I den driftjournal, som bör finnas vid varje driftställe som komplement till befintlig logg, bör noteras de händelser som påverkat driftsituationen. En driftjournal kan föras maskinellt eller manuellt.

Förändringar i driftmiljö, utrustning och rutiner bör ske genom en formell rutin som innebär:

- identifiering och registrering av större ändringar
- konsekvensanalys av sådana ändringar
- godkännande/beslutsform för ändringar
- informationskrav till verksamheten
- rutin för avbrytande av och återställande av misslyckade ändringar.

Vid användning av extern leverantör för drift av informationsbehandlingssystem bör bl.a. följande frågeställningar behandlas:

- identifiering av kritiska tillämpningar som hellre bör hållas inom den egna verksamheten
- godkännande av systemägare
- påverkan på avbrottsplan
- säkerhetsregler och sätt att kontrollera efterlevnad
- övervaknings- och uppföljningsnivå
- incidenthanteringsformer, ansvar, rapportering och hantering.

Driftpersonal (egen och leverantörer) ska vara medvetna om gällande säkerhetsregler och sekretessbestämmelser. För leverantörer ska detta regleras i avtal.

**Tips!**
Se exempel på mall för säkerhetsinstruktion, kontinuitet och drift på KBM:s hemsida (www.krisberedskapsmyndigheten.se).

## 10.2 Kontroll av utomstående tjänsteleverantör

**Mål:** "Att införa och bibehålla lämplig nivå på informationssäkerhet och utförande av tjänster enligt avtal med utomstående leverantör av tjänster."

**Basnivå**

- Rutin ska finnas för hur utomstående leverantörers tjänster följs upp och granskas (Säkerhetsinstruktion, Förvaltning).
- Vid ändring av utförande av utomstående leverantörers tjänster ska en förnyad bedömning av risker göras.

En viktig förutsättning för att kunna bedöma hanteringen av säkerheten i utomstående leverantörers tjänster är att det finns en bra beställarkompetens inom organisationen.

## 10.3 Systemplanering och systemgodkännande

**Mål:** "Att minimera risken för systemfel."

**Basnivå**

- För att säkerställa informationssystems prestanda ska
  - resursanvändningen övervakas och stämmas av
  - planläggning göras för framtida kapacitetskrav
- Informationssystem ska driftgodkännas av systemägaren.
- Vid förändringar i informationssystem ska från fall till fall bedömas om driftgodkännandet måste förnyas.
- Central systemägare ska fastställa vilka gemensamma delar av informationssystemet som ska driftgodkännas centralt samt vilka delar som ska driftgodkännas lokalt och förutsättningarna för detta.
- Informationssystem ska vara överlämnat till förvaltningsorganisation enligt fastställd rutin.
- Acceptanstest ska vara utförd före driftöverlämning.

Driftgodkännande avser den process som utmynnar i ett formellt beslut som fastställer att ett informationssystem i en given miljö uppfyller ställda säkerhetskrav.

För att ett informationssystem ska kunna godkännas för drift måste därför en avstämning göras mot de eventuella krav på generella, ej systemspecifika, åtgärder för informationssäkerheten och för IT-infrastrukturen som kan bli följden av systemsäkerhetsanalysen av informationssystemet.

Ett driftgodkännande kan göras med reservation, vilket innebär att en kortsiktig plan upprättas för de kompletterande säkerhetsåtgärder som ytterligare måste vidtas.

För system som används av flera organisationer sitter systemägaren centralt (central systemägare). Denne ansvarar för granskning av de gemensamma delarna av informationssystemet och för att ett underlag sammanställs för respektive (lokal) systemägare inom övriga organisationer att göra lokala driftgodkännande. Gemensamma delar kan t.ex. vara:

- teknisk plattform
- infrastruktur, nät och nättjänster
- program, applikationer.

Ansvarsgränserna är av stor betydelse, varför underlaget för organisationers driftgodkännande måste innehålla en tydlig gränsdragning mellan centrala och lokala ansvarsområden.

## 10.4 Skydd mot skadlig och mobil kod

**Mål:** "Att skydda riktighet i program och data."

**Basnivå**

- Det ska finnas rutiner för skydd mot skadlig programkod som:
  - minst detekterar förekomsten av sådan
  - kontinuerligt bevakar och implementerar nya uppdateringar både för servrar och klienter
  - startar skyddet automatiskt.
- Rätten att installera nya program, programversioner eller att importera externa filer ska regleras och dokumenteras (Säkerhetsinstruktion, användare och/eller kontinuitet och drift).
- Det ska finnas en rutin för uppdatering av skydd mot skadlig programkod (patch-hantering) för både operativsystem och applikationsprogram.
- Godkänns användning av mobil kod ska regler finnas för detta.

Skyddet mot skadlig programkod måste stå i relation till de skador ett angrepp kan förorsaka. Systemägaren ska därför, i samråd med IT-sidan, göra en bedömning av risken för sådana angrepp och effekterna av dem och utifrån detta vidta åtgärder. Aktuella åtgärder mot skadlig programkod är sådana som bidrar till att, efter upptäckt, förebygga smitta, förhindra smittspridning och återställa smittat system.

Inga program mot skadlig programkod kan garantera ett komplett skydd eftersom nya typer av virus o.dyl. upptäcks kontinuerligt. En viktig del av skyddet är att ha kontroll över vilka program som tillåts i informationssystemet och på vilket sätt information får tillföras detta, t.ex. via datamedia eller Internet. Rätten att installera program, nya versioner av program eller import av externa filer ska därför regleras i driftinstruktionen. Andra möjligheter som bör beaktas för att skydda sig mot skadlig programkod är att dela upp organisationens nätverk i mindre enheter (segmentering), så att en attack enbart drabbar en del av nätverket och att filtrera trafiken via Internet. Program mot virus o.dyl. bör installeras på flera ställen i IT-miljön. Programmen kan vara av två typer, aktiva skydd eller passiva skydd. Den aktiva programvaran startas automatiskt, t.ex. vid uppstart av

arbetsplatsen, och finns sedan i bakgrunden och letar kontinuerligt efter virus och virusliknande aktiviteter. Den kan även kontrollera program och datafiler innan de används. Den passiva programvaran kan aktiveras vid specifika tidpunkter t.ex. vid låg belastning.

Om möjligt bör rutiner som håller servrar och klienter uppdaterade avseende skydd mot skadlig programkod vara automatiserade.

Mobil kod är programkod som överförs från en dator till en annan och sedan exekveras automatiskt. Sådan programkod förekommer idag som applets i webbläsare, som bilagor i elektronisk post samt i annan programvara för uppkoppling mot speciella tjänster över Internet så som internet-bank etc. Mobil kod kan användas för att manipulera eller stjäla information eller för andra illasinnade ändamål.

## 10.5 Säkerhetskopiering

**Mål:** "Att bevara informationens och informationsbehandlingsresursernas riktighet och tillgänglighet."

### Basnivå

- Säkerhetskopiering ska göras regelbundet.
- Systemägaren ska besluta och dokumentera (Säkerhetsinstruktion, kontinuitet och drift):
  - vilken information som ska omfattas av säkerhetskopiering
  - intervallen för kopiering
  - hur många generationer säkerhetskopior som ska finnas
  - hur säkerhetskopior ska förvaras
  - om vissa säkerhetskopior ska förvaras på plats geografiskt skild från driftstället.
- Systemägaren ska besluta om och när kontroll av säkerhetskopiornas läsbarhet ska genomföras och detta ska dokumenteras (Säkerhetsinstruktion, kontinuitet och drift).
- Systemägaren ska besluta om förvaring av och åtkomst till källkod för egenutvecklat informationssystem.
- Åtgärder som ska vidtas för att säkra att informationen är läsbar under hela förvaringstiden ska dokumenteras (Säkerhetsinstruktion, kontinuitet och drift).

- Det ska finnas regler för datamedia (Säkerhetsinstruktion, kontinuitet och drift) för:
  - förvaringstid för datamedia
  - klassning av datamedia
  - hur datamedia ska märkas och förtecknas.
- Test av att informationssystem kan återstartas från säkerhetskopior ska genomföras regelbundet.

Intervallen för säkerhetskopiering bestäms utifrån verksamhetens krav på informationens aktualitet vid återstart från säkerhetskopia. I de flesta fall sker säkerhetskopiering i en för flera informationssystem gemensam driftmiljö av särskilt utsedd personal. I sådana fall måste intervallet för säkerhetskopiering utgå från den verksamhet som har de högst ställda kraven på informationens aktualitet vid återstart. Därför måste intervallet framgå av systemägarens beslut om säkerhetskopiering, men även hur säkerhetskopieringen ska genomföras. Säkerhetskopiering kan omfatta kopiering av all information eller kopiering av de förändringar som skett efter senaste kopieringstillfälle.

När det gäller test av att informationssystem kan återstartas från säkerhetskopior bör sådant helst genomföras åtminstone årligen.

Datamedia kan vara disketter, diskar i servrar, klienter eller minnen i bärbara datorer, men även utskrifter från informationssystem.

Klassning av datamedia måste ta hänsyn till gällande lagar och föreskrifter samt verksamhetens krav, liksom även till det värde som informationen har för verksamheten. Även andra intressenters specifika krav måste beaktas. Klassningen avgör vilka datamedia som ska omfattas av särskilda förvaringsrutiner.

Exempel på bestämmelser som styr vad som ska gälla för förvaringstid av information lagrad på media är arkivlagen och Riksarkivets författningssamling. Se vidare Sveriges Provnings-och Forskningsinstituts (SP) information.

## 10.6 Hantering av säkerhet i nätverk

**Mål:** "Att säkerställa skyddet av information i nätverk och i tillhörande infrastruktur."

**Basnivå**

- Det ska finnas en ansvarig person för varje del av i nätverket ingående nätsegment.
- Nätadministrationen ska skiljas från ordinarie administration och underhåll av informationssystem.
- Det ska vara möjligt att logga säkerhetsrelevanta händelser.
- Korskopplingsskåp ska vara låsta.

Administrationen av bryggor och routrar m.m. bör vara knuten till ansvaret för övriga delar av nätet. Nätadministratören bör ha ansvar för att t.ex. konfigurera servrar, routrar och namnservrar och arbeta tillsammans med säkerhetspersonal för att upprätthålla säkerheten i nätet. Dessutom bör åtminstone en ersättare vara utsedd, som har tillräckliga kunskaper för att vid behov kunna träda in i den ordinaries ställe. Åtkomstkontrollen bör bygga på säkerhetsdomäner. En domän bör vara ett visst verksamhetsområde som omfattar vissa informationssystem och användare som lyder under samma säkerhetsregler och som har en gemensam säkerhetsadministration.

Regler för anslutningar mellan säkerhetsdomäner bör innehålla information om möjliga trafikriktningar, protokolltyper och tjänster. Normalt ska inte samtliga administratörer ha fullständiga systembehörigheter utan endast vad som krävs för att fullgöra sina arbetsuppgifter. Routingtabeller etc. måste skyddas mot obehörig insyn och förändring genom lösenord eller motsvarande. Det behöver inte ställas krav på upprepad autenticering av användare, när de använder nätapplikationen, om autenticeringen ägt rum vid arbetsstationen. Nätapplikationen kan få information om användaridentiteter genom data från klientapplikationen eller genom att identifiera nätadressen.

Följande ska beaktas särskilt:

- driftansvar för nätverk bör där det är möjligt vara skilt från ansvar för övrig drift
- ansvar och rutiner ska fastställas för hantering av all ingående utrustning i nätverket
- särskilda skyddsåtgärder ska beaktas för att skydda sekretess och riktighet när data passerar allmänna nät liksom skydd av anslutna system och utrustning.

Det är viktigt att skydda multimaskiner, skrivare mm. som tillhör nätverket mot obehörig åtkomst.

## 10.7 Hantering av media

**Mål:** "Att förhindra obehörigt avslöjande, modifiering, borttagning eller förstörande av tillgångar och avbrott i organisationens verksamhet."

**Basnivå**

- Systemägaren ska fastställa vilken information, lagrad på datamedia, som ska omfattas av särskilda förvaringsrutiner så att den inte kan läsas av obehöriga.
- Det ska finnas regler för förvaringstid för datamedia (Säkerhetsinstruktion, kontinuitet och drift).
- Datamedia, med för verksamheten väsentlig information, ska förvaras i utrymme som är konstruerade för ändamålet.
- Datamedia och säkerhetskopior av dessa ska förvaras i olika brandceller eller särskilt utformade förvaringsutrymmen.
- Det ska finnas regler för hur datamedia med sekretessbelagd information ska avvecklas (Säkerhetsinstruktion, förvaltning).
- Systemägaren ska besluta hur lagringsmedia med informationssystemets information ska avvecklas.

För att kunna bedöma vilka datamedia som ska skyddas mot obehörig åtkomst måste informationen som lagras på dessa datamedia klassas. Av säkerhetsinstruktionen ska framgå hur sådan datamedia ska förvaras, exempelvis om säkerhets- eller värdeskåp ska användas. Datamedia bör förvaras i skåp eller motsvarande utrymme som svarar upp mot minst brandklass D60 eller motsvarande. För utrymme eller skåp där säkerhetskopior förvaras måste brandlagen samt eventuella föreskrifter från försäkringsinstitut beaktas.

Systemägaren beslutar vilka förvaringsutrymmen som får användas. Det bör finnas särskilt tillträdesskydd till utrymme där datamedia förvaras, t.ex. säkerhetsskåp.

Det finns risk för att informationsmedia som fysiskt transporteras, exempelvis via post eller bud, kan utsättas för obehörig åtkomst, missbruk eller förvanskning. En bedömning måste därför göras, utifrån känsligheten i informationen, av hur datamedia ska emballeras, fysiskt förflyttas och av vem. Användning av kryptering och elektronisk underskrift bör övervägas.

Flyttbara datamedia ska hanteras så att:

- tidigare innehåll från återanvändbara media som inte längre behövs ska raderas innan de lämnar organisationen, t.ex. genom överskrivning med teknik som motsvarar kraven för aktuell klassificeringsnivå.
- alla media som lämnar organisationen förtecknas för att bibehålla spårbarhet.
- förvaring sker på säker plats och i lämplig miljö enligt tillverkarnas specifikationer.

## 10.8 Utbyte av information

**Mål:** "Att bibehålla säkerheten hos information och programvara som utbyts inom organisationen och med någon extern enhet."

**Basnivå**

- Det ska finnas dokumenterade regler (Säkerhetsinstruktion, användare) för:
  - vilken information som får skickas med elektronisk post
  - filöverföring via elektronisk post som minst omfattar virus-kontroll av meddelanden och bifogade filer.
- Systemägarens ansvar vid dataöverföring till och från informationssystemet ska klargöras.
- Informationsutbyte mellan system utanför organisationen ska regleras i avtal.
- Det ska finnas en rutin för godkännande av publicering av information i system som är allmänt tillgängliga.
- Systemägaren ska besluta vilka åtgärder som ska vidtas vid fysisk transport av för verksamheten känslig information (Säkerhetsinstruktion, förvaltning).
- Regler ska finnas för att skydda information som delas av flera informationssystem
- Internettjänster får ej driftsättas utan godkända säkerhets-funktioner.
- Anvisningar för säkerhetsfunktioner vid utveckling av webbtjänster mot allmänheten ska dokumenteras (Säkerhetsinstruktion, förvaltning).

De regler som gäller för vilken information som får skickas med elektronisk post bör minst omfatta klassificering av informationen med utgångspunkt från lagstiftningens och verksamhetens krav. De bör även innehålla regler för:

- vilken information som ska krypteras och vilken som ska ha elektronisk underskrift
- kryptering, nyckelhantering och nyckelöverföring
- nätövervakning, kontroll av angrepp och behörighetskontrollsystem

- val av standardprotokoll och datakommunikationsalternativ
- funktioner för användarstöd inom organisationen.

För drift av organisationens interna e-postsystem bör gälla att det interna e-postsystemet isoleras från externa nät, t.ex. genom någon form av brandväggsfunktion.

För att undvika problem med ökad risk för sekretessbrott, virusspridning och onödig belastning av systemresurser bör följande beaktas:

- automatisk vidarekoppling bör inte vara tillåten om risk att känslig information förmedlas oskyddat (t.ex. personuppgifter)
- restriktivitet när det gäller att skicka eller vidarebefordra meddelanden som innehåller stora filer
- försiktighet vid öppnande av bifogade filer.
- om misstanke att det kommit in virus via e-postsystemet ska kontakt tas med anvisad stödfunktion.

Systemägaren måste ha klart för sig vad dennes ansvar vid dataöverföring till och från informationssystemet innebär, exempelvis i händelse av förlust eller förändring av data eller avseende säkerhetsåtgärder vid sändning/mottagning av data. Om dataöverföring sker mellan två organisationer med skilda ansvar måste en samverkan i säkerhetsfrågor mellan de båda systemägarna och mellan dessa och nätoperatören ske. Ansvarsfrågorna kompliceras av att dataöverföringen ofta sker med hjälp av kommunikationslinjer och annan kommunikationsutrustning över vilka systemägaren inte förfogar. En separat nätoperatör har ofta ansvaret för att överföringen tekniskt fungerar i enlighet med överenskomna specifikationer. Detta innebär också att nätoperatören är ansvarig för de säkerhetsåtgärder som behövs för att skydda utrustningen i nätet. Nätoperatören är i sin tur beroende av att nätägaren upprätthåller en god säkerhet. Den säkerhetsnivå som definieras av systemsäkerhetsanalysens krav på ett informationssystem ställer också indirekta krav på eventuella externa kommunikationer och kommunikationstjänster. Systemägaren behöver kännedom om vilka säkerhetskrav som tekniken och köpta kommunikationstjänster kan uppfylla och om kompletterande egna åtgärder måste vidtas. Alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket måste undvikas. En aktuell förteckning över samt-

liga anslutningar gör det möjligt att regelbundet identifiera dem som godkänts. Att anslutningar inte otillåtet etablerats kan då kontrolleras. Detta inkluderar även alla former av anslutningar för underhåll och service av leverantörer och eventuell fjärrdiagnostik.

Det finns olika typer av autenticeringsmetoder med olika grad av skydd. Val av metod görs mot bakgrund av riskanalyser. Bland olika metoder märks sådana som baseras på krypteringsteknik, aktiva kort, utnyttjande av anrops/svarsprotokoll och motringningsrutiner.

I elektroniska publiceringssystem och system för elektroniska tjänster (Internet), särskilt sådana som tillåter återrapportering och direktinmatning av information, bör säkerställas att:

- information inhämtas och behandlas i enlighet med bestämmelser i lagstiftning rörande personuppgifter
- information som inmatas till och bearbetas av publiceringssystemet kommer att bearbetas fullständigt, korrekt och i rätt tid
- känslig information som inmatas i systemet skyddas under överföring och lagring
- åtkomst till publiceringssystemet inte tillåter icke avsedd åtkomst till nätverket i övrigt och inte heller till andra nätverk till vilka länkar finns.

Rutiner och styrmedel bör finnas för att skydda informationsutbyte genom användning av röst-, fax- och videokommunikationsutrustning.

Informationsutbytet som regleras i avtal bör reglera såväl nyttjanderättsfrågor, ekonomiska frågor samt krav på säkerhet som gör att båda parters behov av sekretess, riktighet och tillgänglighet kan upprätthållas.

## 10.9 Elektronisk handel

**Mål:** "Att säkerställa säkra e-handelstjänster och en säker användning av dessa."

**Basnivå**

- För elektronisk handel ska samma säkerhet gälla som för utbyte av information i övrigt

## 10.10 Övervakning

**Mål:** "Att upptäcka obehörig informationsbehandling."

**Basnivå**

- Det ska finnas revisionsloggar för säkerhetsrelevanta händelser som minst registrerar
  - användaridentitet
  - datum och tidpunkt för in- och utloggning
  - lyckade och misslyckade försök till åtkomst
- Det ska finnas administratörs- och operatörsloggar som minst registrerar
  - konto och involverad administratör/operatör
  - vilka processer som involverats
  - datum och tidpunkt för in- och utloggning
  - lyckade och misslyckade försök till åtkomst
- I de fall administratörs-/operatörsåtgärder inte möjliga att logga automatiskt ska manuell logg föras.
- Systemägaren ska fastställa vilka händelser utöver ovanstående som ska registreras i informationssystemets logg.
- Central systemägare ska säkerställa att informationssystemet är konstruerat så att revisionsloggar finns för säkerhetsrelevanta händelser som minst registrerar
  - användaridentitet
  - datum och tidpunkt för in- och utloggning
  - lyckade och misslyckade försök till åtkomst

- För informationssystems loggar ska systemägaren besluta (Säkerhetsinstruktion, förvaltning):
  - hur ofta de ska analyseras
  - vem som ansvarar för analyser av dem
  - hur länge de ska sparas
  - hur de ska förvaras.
- Anvisningar för organisationens användning och övervakning av loggfiler vid drift ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Loggar ska
  - bevaras under tid som i enlighet med gallringsbeslut som även ska tillgodose behov av utredning av incidenter.
  - kontrolleras regelbundet med avseende på tecken på onormala förhållanden och säkerhetsincidenter.
- Rutin ska
  - finnas för hur informationssystems loggar övervakas.
  - innehålla instruktioner om hur felmeddelanden och annan information ska tas omhand, vilka som ska informeras etc.
- Loggningsresurser och logginformation ska skyddas mot obehörig åtkomst och manipulering
- Klockorna i informationssystemen måste synkroniseras med en godkänd exakt tidsangivelse.

Vid uppföljning av säkerhetshändelser via loggar är det mycket viktigt att datorklockor är synkroniserade. Användning av NTP (Network Time Protocol) via internetoperatören (ISP) bör övervägas.

Med spårbarhet menas möjligheten att via registreringar identifiera och följa förloppet för olika händelser. En samordning av flera loggar kan behövas för att få den spårbarhet som är loggningens egentliga syfte.

För att kunna genomföra spårningen i ett informationssystem behövs kunskap om systemets bearbetningar och den kronologiska ordningen för dem. Hjälpmedlen för detta är en eller flera bevakningsfunktioner i form av loggning. För varje system ställs kravet på möjligheter till spårbarhet i relation till informationens skyddsvärde.

Säkerhetsloggarna bör följas upp kontinuerligt. En analys av dem ska inriktas mot alla former av överträdelser mot gällande regler.

Normalt räcker det att spara säkerhetsloggar i två år, men i vissa fall kan de av särskilda orsaker behöva sparas längre. Exempelvis ska loggar avseende ekonomisystem och ekonomitransaktioner lagras i 10 år, så att Bokföringsförordningens krav på spårbarhet och återskapande kan efterlevas. Förutsättningar måste då finnas för att kunna läsa informationen under den tid som loggarna sparas.

Loggar som registrerar avvikelser och andra säkerhetsrelevanta händelser bör omfatta:

- användaridentitet
- datum och tidpunkt för på- och avloggning
- om möjligt, terminalidentitet och -placering
- registrering av lyckade och misslyckade försök till systemåtkomst
- registrering av lyckade och misslyckade försök till åtkomst av data och andra resurser.

Loggar ska omfatta driftoperatörs- och systemadministratörsåtgärder och bör omfatta:

- start- och sluttid för drift av system
- systemfel och vidtagna korrigerande åtgärder
- bekräftelse av korrekt driftresultat i fråga om filer och utdata
- namnet på den person som för in uppgift i loggen vid manuell loggning.

För vissa informationssystem kan det vara viktigt att vid en eventuell juridisk process bevisa att loggar inte är förändrade. I sådana fall bör man överväga att signera aktuella loggar.

# 11. Styrning av åtkomst

## 11.1 Verksamhetskrav på styrning av åtkomst

**Mål:** "Att styra åtkomst till information."

**Basnivå**

- Om möjligt ska användare ges en behörighetsprofil som endast medger den åtkomst till aktuellt informationssystem som krävs för att lösa arbetsuppgifterna.
- Systemägaren ska fastställa vilka och vilken typ av anslutningar till tele- och datanät som ska tillåtas.
- Beslut om anslutningar till tele- och datanät ska dokumenteras.
- Det ska finnas en aktuell förteckning över samtliga externa anslutningar.
- Det ska regelbundet kontrolleras vilka uppkopplingar som finns mot ett informationssystem.

## 11.2 Styrning av användares åtkomst

**Mål:** "Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem."

**Basnivå**

- Endast utsedd behörig ska ha rätt att installera nya program i nätverket.
- Det ska finnas särskild behörighet till nätverket utöver den för respektive applikation.
- Systemadministratörer/-tekniker ska alltid ha individuella användaridentiteter.

- Behörighetsregister ska endast vara åtkomligt för utsedd administratör.
- Antalet konton med privilegierade rättigheter och omfattningen av dessa rättigheter ska minimeras.
- Samtliga administratörer ska inte ha fullständiga systembehörigheter, utan endast i den utsträckning som krävs för arbetsuppgifterna.
- Routingtabeller etc. ska endast vara åtkomliga för behöriga administratörer.
- Det ska finnas en dokumenterad (Säkerhetsinstruktion, förvaltning) rutin för tilldelning, uppföljning och uppdatering av behörighet.
- Systemägaren ska fastställa vem som har rätt att besluta om behörighet.
- Det ska finnas dokumenterade rutiner för hantering av behörighet för användare som slutar eller byter arbetsuppgifter (Säkerhetsinstruktion, förvaltning).
- Nya användare ska ges ett initialt lösenord som de ska byta till ett eget valt lösenord vid första användning.
- Före tilldelning av behörighet ska användare ges tillräckliga kunskaper om:
  - de säkerhetsinstruktioner som generellt gäller för IT-verksamheten
  - de instruktioner som speciellt ansluter till den egna arbetsuppgiften.
- Behörighet som upphört att gälla ska spärras inom högst en vecka.
- Minst en gång per år ska kontrolleras att endast behöriga användare är registrerade i behörighetssystemet
- Endast utsedd administratör ska kunna registrera, förändra eller ta bort användares åtkomsträttigheter.
- Det ska finnas utsedd personal i reserv och eventuella reservrutiner för hantering av behörighet.

- Behöriga användare av informationssystem ska vara registrerade i ett behörighetskontrollsystem med de rättigheter som beslutats. Om möjligt ska användare ges en behörighetsprofil som endast medger den åtkomst till aktuellt informationssystem som krävs för att lösa arbetsuppgifterna.
- För lösenord ska gälla att:
  - varje användare ska ha en unik användaridentitet och ett lösenord som endast denne känner till och kan ändra
  - de ska bestå av minst 8 tecken för såväl användare som systemadministratörer/-tekniker och vara konstruerade så att de inte lätt går att pröva sig fram till eller gissa
  - användarna ska tvingas byta lösenord enligt tidsintervall som systemägaren beslutar
  - högst tre felaktiga inloggningsförsök ska tillåtas innan användarkontot låses
  - de inte ska tillåtas återanvändas inom en tidsrymd som bestäms av säkerhetssamordningsfunktionen och som inte underskrider tretton månader.
- För arbetsstation ska gälla att:
  - användare som lämnar den obevakad ska aktivera skärmsläckare med automatisk låsning
  - upplåsning ska ske med lösenord
- Låst användarkonto ska öppnas först efter säker identifiering av användaren.
- Lagrade lösenord ska skyddas genom kryptering.
- Det ska finnas rutiner som förhindrar att standard- eller leverantörsbehörigheter kan användas.
- För informationssystem med central systemägare ska denne säkerställa att det är konstruerat så att alla rekommendationer på basnivå avseende behörighetskontroll kan tillgodoses.

Med behörighet avses en användares rättighet att på ett reglerat sätt utnyttja ett informationssystem och dess resurser. För att uppnå detta krävs samverkande tekniska och administrativa åtgärder. Med behörighetskontroll avses administrativa och tekniska åtgärder för kontroll av användares identitet, för styrning av användares behörighet samt för uppföljning av användning. Sådan kontroll sker vanligen i ett

behörighetskontrollsystem som möjliggör verifiering av identiteten, reglering av åtkomsträttigheter samt registrering av användarens aktiviteter i informationssystemet (loggning). Ett lösenord bör bestå av en blandning av bokstäver, siffror och specialtecken för att försvåra möjligheterna att avslöja det. Beslut om behörighet bör dokumenteras och sparas.

Som en extra åtgärd för att förvissa sig om att arbetsstationer inte står öppna beroende på att användare glömt att aktivera skärmsläckaren, kan övervägas att införa en generell tidsperiod för automatisk aktivering av skärmsläckare.

Användare bör inte ha administratörsrättigheter på sina maskiner och möjlighet att installera program själva eller ha åtkomst till operativsystem och systemverktyg.

## 11.3 Användares ansvar

**Mål:** "Att förhindra obehörig användaråtkomst och åverkan eller stöld av information och informationsbehandlingsresurser."

### Basnivå

- Användare ansvarar för att:
  - inte avslöja sitt lösenord för andra eller låna ut sin behörighet
  - skydda lösenordet väl
  - omedelbart byta lösenordet om det kan misstänkas att någon annan känner till det
  - byta lösenordet enligt reglerna
  - inte återanvända tidigare lösenord
  - ej använda samma lösenord externt.
- Informationsbehandlingsutrustning i publikt utrymme ska
  - vara fastlåst
  - endast medge att avsedda publika tillämpningar kan nås från den.
- Pappersdokument och lagringsmedia i användares arbetsrum måste hanteras i enlighet med hur informationens klassning.

## 11.4 Styrning av åtkomst till nätverk

**Mål:** "Att förhindra obehörig åtkomst till nätverkstjänster."

### Basnivå

- Brandväggsfunktionen ska vara den enda kanalen för IP-baserad datakommunikation till och från organisationen.
- Ansvaret för administration av brandväggen ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Brandväggens utformning och konfiguration ska dokumenteras.
- Brandväggen ska vara försedd med skydd mot skadlig programkod.
- Nätverkets systemägare ska, i samråd med respektive systemägare, besluta (Säkerhetsinstruktion, förvaltning):
  - vad som ska loggas i brandväggen
  - vem som ansvarar för uppföljningen av loggarna
  - hur ofta uppföljning ska ske
  - hur länge loggarna ska sparas.
- Används trådlösa lokala nät, ska nätverkets systemägare besluta om åtgärder mot obehörig avlyssning och utnyttjande ska vidtas.
- Servrar ska skyddas genom behörighetskontrollsystem i operativsystemet eller genom att endast ge användarna tillgång till servern via en nätapplikation.
- Det ska finnas dokumenterade regler för vad som är tillåtet för anslutningar mellan säkerhetsdomäner.
- Om fjärrdiagnostik används ska sådan ske enligt fastställda rutiner.
- Utifrån systemägarens krav ska behovet av autenticeringsmetod vid externa anslutningar klarläggas.
- Det ska finnas regler för hur autenticering ska ske vid externa anslutningar (Säkerhetsinstruktion, förvaltning).
- Säkerhetsarkitekturer för interna och externa nät och kommunikationssystem ska dokumenteras (Säkerhetsinstruktion, förvaltning
- Det ska finnas dokumenterade regler för anslutning av utrustning till interna och externa nätverk (Säkerhetsinstruktion, förvaltning)

- Regler och rutiner för anslutning av externa nätverk till organisationens eget nät med ingående säkerhetsfunktioner, autenticering etc. ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Anvisningar för anslutning av trådlösa nätanläggningar ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Anvisningar för säkerhet vid Internetanslutning ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Administratörens förehavanden ska loggas och inte kunna förändras eller raderas.
- Uppkoppling mot Internet får endast ske då det verifierats att säkerhetsfunktionerna är i drift.

Som regel är brandväggen en gemensam resurs för en organisation vilket innebär att dess säkerhetsnivå måste ta hänsyn till säkerhetskrav från flera verksamhetsområden. Exempel på frågeställningar som kan vara aktuella när policyn för en brandvägg ska utformas är följande:

- vilka tjänster ska brandväggen tillhandahålla
- vilka uppgifter ska döljas av brandväggen, exempelvis strukturen på det egna nätet, egna ip-adresser och användaridentitet
- vad ska loggas i brandväggen
- ska e-post kontrolleras i brandväggen
- ska viruskontroll ske i brandväggen
- vilken kontroll ska ske av Internetaccess/loggning
- krävs integritetskontroll av brandväggsprogramvara
- vilket fysiskt skydd behövs för brandväggen (begränsad tillträdeszon)
- hur ska brandväggsadministrationen ordnas
- vilken autenticeringskrav ska gälla för brandväggen, t.ex. vid fjärråtkomst (remote access)
- vad ska säkerhetskopieras.

Allt fler organisationer bygger upp trådlösa nät för sin verksamhet, s.k. WLAN (Wireless Local Area Net). För trådlösa nätverks infrastruktur finns inte bara behov av autenticering av klienter utan klienter bör även kräva autenticering av infrastrukturen.

Standarderna för trådlösa nät innehåller en säkerhetslösning som omfattar såväl autenticering och kryptering som integritetskontroll. Denna säkerhetslösning kallas WEP (Wired Equivalent Privacy). WEP är ingen heltäckande säkerhetslösning utan bör kombineras med andra lösningar.

Accesspunkter i trådlösa nät bör stängas av under perioder de inte används.

Säkerhetsarkitekturer för interna och externa nät och kommunikationssystem bör omfatta tekniska anvisningar för:

- åtkomst till e-post, filöverföringar och datum/tid för åtkomst till nätverk
- uppdelning av nätverk
- krav mot extern leverantör av extern nätverkstjänst
- säkerhetsarkitektur för användning av trådlösa kommunikationsnät.

Möjlighet till automatisk nerkoppling av internetkommunikation vid exceptionella händelser bör övervägas.

## 11.5 Styrning av åtkomst till operativsystem

**Mål:** "Att förhindra obehörig åtkomst till operativsystem."

**BASNIVÅ**

- Inloggningsrutinen
  - ska inte visa identitetsbegrepp för system eller tillämpningar förrän fullständig inloggning lyckats.
  - ska inte lämna meddelanden under inloggningsrutinen som skulle kunna hjälpa en obehörig användare.
  - ska validera inloggningsinformationen först sedan alla data inmatats.
  - ska registrera misslyckade försök i logg
- Regler ska finnas för systemhjälpmedel som kan förbigå system- och tillämpningsspärrar (Säkerhetsinstruktion, förvaltning)
- Sessioner ska automatiskt kopplas ned efter en definierad period av inaktivitet.
- För känsliga tillämpningar ska begränsningar finnas för uppkopplingstid

Arbetsstationer bör ha en i nätverket unik identitet som ger en rimlig kontroll av anslutningen. Eventuella undantag bör godkännas först efter genomförd riskanalys. Undantag bör inte medges för system med information i högsta sekretess- och riktighetsklass eftersom krav på spårbarhet och oavvislighet då finns.

Användning av administrationsverktyg eller systemhjälpmedel som kan förbigå system- och tillämpningsspärrar bör begränsas och styras. Dokumenterade regler bör finnas för hur och när de får användas. Loggning bör göras av all användning av dessa verktyg/hjälpmedel.

Konsolterminal ska ha fysiskt skalskydd på samma nivå som den dator konsolen styr.

Användning av begränsningar i uppkopplingstid ska övervägas för tillämpningar med hög risk för obehörigt utnyttjande.

## 11.6 Styrning av åtkomst till information och tillämpningar

**Mål:** "Att förhindra obehörig åtkomst av information i tillämpningar."

### Basnivå

- Det ska finnas definierade regler för åtkomst som beaktar att åtkomst ska
  - som grundregel begränsas med utgångspunkt från behovet att kunna utföra en arbetsuppgift
  - ges med hänsyn till hur information klassificeras.
  - kunna spåras om informationens klassificering kräver det.
  - inte kunna ske anonymt vid användning av informations-behandlingsresurs.
  - kunna styras med olika åtkomsträttigheter
  - beslutas och dokumenteras.
- Endast behöriga personer ska ha tillgång till media med för verksamheten väsentlig information.
- Systemet ska vara kopplat till de behörighetskontrollfunktioner som tillämpas inom organisationen.
- Det ska inte vara möjligt att komma åt databaser med hjälp av andra tjänster än de avsedda.

Följande bör beaktas när det gäller styrning av åtkomst till tillämpningar:

- information som tillhör organisationen lagras i anvisade system eller på därför avsedda kataloger i filservrarna.
- lagring av organisationens information på lokala hårddiskar får ske endast om kopia finns på filservrarna.
- användare av bärbar PC har skyldighet att se till att organisationen tillhörig information som lagras lokalt kopieras till filservrarna.
- bärbar PC får ej vara uppkopplad mot extern organisations datanät samtidigt som den är uppkopplad mot organisationens nät.
- användare som hanterar information lokalt ska vara medveten om informationens sekretessklassificering och hantera informationen enligt detta.

Följande principer bör övervägas för behörighetsstyrning:

- system ska i första hand konstrueras så att behörighet knyts till användaridentiteten både för att avgöra vilka funktioner inom systemet användaren ska ha tillgång till och vid access i fleranvändardatabas.
- i andra hand ska styrning av vilka funktioner inom systemet användaren ska ha tillgång till och av access i fleranvändardatabas göras med för systemet särskilt definierad accessidentitet. Denna identitets lösenord ska lagras så att det skyddas mot avläsning.

## 11.7 Mobil datoranvändning och distansarbete

**Mål:** "Att säkerställa informationssäkerheten vid användning av mobil utrustning och utrustning för distansarbete."

**Basnivå**

- Kraven på teknisk säkerhet och praktisk hantering av mobil utrustning ska dokumenteras (Säkerhetsinstruktion, användare).
- Systemägaren ska besluta om ett informationssystems information ska få bearbetas på distans med stationär eller mobil utrustning.

Det är allt vanligare förekommande att anställda arbetar utanför organisationens lokaler, i hemmet eller på annan plats. Hantering av bärbara datorer och annan mobil utrustning och dess uppkoppling mot det interna nätverket måste regleras. Det kan därvid vara lämpligt att upprätta avtal med aktuella användare för vad som ska gälla för distansarbete. Speciell försiktighet måste iakttas när det gäller distansarbete från hemmet samt vid användning av mobil utrustning som laptops, handdatorer, mobiltelefoner o.dyl. på plats geografiskt skild från organisationens arbetslokaler.

Frågor som kan vara aktuella att reglera för distansarbete kan exempelvis gälla följande:

- fysiskt skydd i eller utanför hemmet (stöldrisk, brandrisk)
- logiskt skydd (otillbörlig användning)
- om utrustningen endast får användas för arbetsgivarens arbete (virussmitta o.dyl.)
- hantering av utskrifter (obehörig tillgång)
- om lagring och säkerhetskopiering av information ska ske i egen dator eller hos arbetsgivaren (stöldrisk, obehörig tillgång och förstörelse m.m.)
- hur eventuella hjälpinsatser utifrån (remote) ska ske (obehörigt intrång)
- kontroll av skadlig programkod (virussmitta o.dyl.)
- om kryptering krävs vid överföring i vissa fall (obehörig tillgång och förändring)
- autenticering vid uppkoppling mot arbetsgivarens nätverk (obehörig tillgång och förändring)

Det kan finnas skäl att överväga att införa kontroll av klienter att de har uppdaterade antivirusprogram och inlagda säkerhetspatchar mm. innan de släpps in på det interna nätverket.

# 12. Anskaffning, utveckling och underhåll av informationssystem

## 12.1 Säkerhetskrav på informationssystem

**Mål**: "Att säkerställa att säkerheten är en integrerad del av informationssystemet."

### Basnivå

- En systemsäkerhetsanalys ska:
  - upprättas för varje informationssystem som bedöms viktigt för verksamheten
  - fastställas av systemägaren och dokumenteras
  - utpeka vem som är systemägare
  - innehålla de samlade kraven på säkerhet som ställs på informationssystemet
  - vara avstämd mot informationssäkerhetspolicyn och gjorda policyuttalanden.
- Det ska finnas dokumenterade, av ledningen beslutade, säkerhetsinstruktioner för förvaltning (Säkerhetsinstruktion, förvaltning)
- Om publika nät utnyttjas inom ramen för informationssystemet ska systemägaren ska ta ställning till om nätoperatörens tjänster uppfyller verksamhetens säkerhetskrav.
- Informationssystem som tas i bruk ska ha stämts av mot de säkerhetskrav som verksamheten ställer.

För att kunna bedöma säkerhetskraven på ett informationssystem är det nödvändigt att klarlägga vilka verksamheter som systemet stöder, hur beroende de är av det och vilka krav som ska ställas på det.

I systemsäkerhetsanalysen klarläggs vilka säkerhetskrav som ska ställas för att:

- förhindra eller försvåra för en obehörig att få tillgång till informationen (sekretess)
- säkerställa att den information som produceras och bearbetas i informationssystemet är korrekt, aktuell och fullständig (riktighet)
- att informationssystemets funktion och information är åtkomlig vid behov (tillgänglighet).

Riskanalysen baseras på bedömningar av vilka hot som finns mot informationssystemet, sannolikheten för att de realiseras och vilka konsekvenser detta skulle få för verksamheten.

Rutiner för behörighetsadministration, rutiner för införande, förvaltning och avveckling av system, olika systemadministrativa åtgärder knutna till informationsbehandlings- och kommunikationsresurser o.dyl. klarläggs i Säkerhetsinstruktion, förvaltning.

Det är viktigt att redan i utvecklings- och inköpsfasen av ett informationssystem utreda säkerhetskraven på systemet samt behovet av reservrutiner för detta. Detta gäller även vid större förändringar av befintliga informationssystem. Rutiner för detta är därför angelägna. De kan avse sådant som kraven på certifierade och evaluerade produkter, tester, testmiljö, tidpunkter för tester och införande m.m.

Utgångspunkten bör vara att köpta system och program ska vara certifierade av ett oberoende organ eller att de är framtagna och utgivna av betrodda leverantörer.

Rutiner för inköp och installation av program är särskilt viktiga i nätmiljöer. Risken för att t.ex. datavirus överförs till andra miljöer i det lokala nätet är överhängande om en arbetsplats har blivit smittad.

## 12.2 Korrekt bearbetning i tillämpningar

**Mål:** "Att förhindra fel, förlust, obehörig förändring eller missbruk av information i tillämpningssystem."

**Basnivå**

- Regler ska finnas för validering
  - av informationssystems in- och utdata (Säkerhetsinstruktion, förvaltning)
  - för att upptäcka förvanskning av information
- Det ska finnas dokumenterade regler för rättning av data (Säkerhetsinstruktion, kontinuitet och drift).
- Persondata som förmedlas över öppna nät ska krypteras.

Regler för rättning av data bör minst omfatta:

- vem som är ansvarig för datakvaliteten
- hur ofta kontroller ska genomföras.

## 12.3 Kryptering

**Mål:** "Att skydda informationens sekretess, autenticitet eller riktighet med kryptering."

**Basnivå**

- Finns beslut om kryptering av information ska regler för detta dokumenteras (Säkerhetsinstruktion, förvaltning).
- Anvisningar för tillämpning av kryptering ska dokumenteras (Säkerhetsinstruktion, förvaltning).
- Regler för nyckelhantering ska finnas om krypteringsteknik används.

Behovet av krypteringsteknik inom en organisation bör övervägas utifrån genomförda riskanalyser. I de fall ett sådant behov föreligger, bör organisationen utveckla regler för kryptering för att undvika olämplig eller felaktig användning.

Kryptering bör användas inom organisationen samt vid extern uppkoppling till/från organisationens nät i de fall data eller information ställer höga krav på:

- skydd mot obehörig avlyssning,
- skydd mot obehörig insyn,
- skydd mot obehörig förändring,
- skapande av elektronisk underskrift och
- säker autenticering (stark autenticering)

Beprövade eller evaluerade produkter för kryptering ska användas.

Anvisningar för nyckelhantering utformas av driftorganisationen i samråd med funktionen för informationssäkerhetssamordning.

## 12.4 Säkerhet i systemfiler

**Mål:** Att säkerställa säkerheten i systemfiler.

**Basnivå**

- Det ska finnas regler för installation av programvaror i system som är i drift.
- Testdata ska kontrolleras och skyddas.
- Åtkomst till källkod ska begränsas.

Införande av nya program i befintliga system ska följa dokumenterad process/rutin. Införande får endast ske om beslutad testprocess genomgåtts som också innefattar test av säkerhetsfunktioner (systemgodkännande).

Testdata bör skyddas och kontrolleras. Att använda produktionsdatabaser med verkliga persondata är inte tillåtet. Personuppgifter ska anonymiseras före användning som testdata.

Följande kontroller bör tillämpas för att skydda produktionsdata om de används för teständamål:

- rutiner för styrning av åtkomst som tillämpas för produktionssystem bör också gälla vid test av sådana system.
- behörighet bör ges särskilt varje gång produktionsdata kopieras till ett testsystem.

- produktionsdata bör raderas från testsystem genast efter avslutad test.
- kopiering av produktionsdata bör loggas för att få spårbarhet.

## 12.5 Säkerhet i utvecklings- och underhållsprocesser

**Mål:** "Att bibehålla säkerheten i tillämpningssystemens program och information."

### Basnivå

- Det ska finnas utsedda systemadministratörer.
- Det ska finnas personal med ansvar för systemunderhåll.
- I avtal ska regleras hur känslig information ska hanteras i samband med service.
- Fjärrdiagnostik ska ske under kontrollerade former.
- Det ska finnas regler för hur system- och programutveckling ska genomföras (Säkerhetsinstruktion, förvaltning).
- Beslut om programändringar ska fattas av systemägaren.
- Systemägaren fattar beslut om tidpunkt för installation av nya programversioner.
- Utveckling och förändringar i program ska dokumenteras.
- Det ska finnas rutiner för hur kunskap om förvaltning ska återföras till den egna organisationen för egenutvecklade program som utvecklats externt.
- Det ska finnas rutiner för hur utbildning ska genomföras för köpta system, som även ska omfatta kompletterande utbildning vid program- och funktionsändringar.
- Tillgången till egenutvecklade informationssystems källkod ska regleras i avtal.
- Upphovsrättsliga frågor ska vara reglerade i avtal.
- Det ska finnas systemdokumentation för ett informationssystem som omfattar:
  - vad informationssystemets olika delar består av
  - övergripande beskrivning av de olika delarnas uppgift
  - en detaljerad systembeskrivning.

- En kopia av systemdokumentationen i sin helhet ska förvaras väl skild från originalet.
- Systemdokumentation med känslig information ska endast vara åtkomlig för behörig personal.
- Det lokala nätverket, dess ingående komponenter och varje förändring av det ska dokumenteras.
- All dokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i informationssystem.
- Alla programvaror som ska kunna installeras på standardarbetsplats (arbetsstation) ska vara testad och godkänd så att de inte stör övriga funktioner i standardarbetsplats eller gemensamt datanät.
- Installationsanvisningar och i förekommande fall, rutiner för programdistribution, ska vara upprättade.

I systemunderhåll ingår att kontinuerligt styra och ändra informationssystem i syfte att säkerställa dess kvalitet och nytta i verksamheten. Normalt bör förbindelse för fjärrdiagnostik vara nerkopplad och endast kopplas upp efter direkt överenskommelse vid varje enskilt tillfälle.

Förvaltningsinstruktion för utveckling bör omfatta:

- ansvar för systemutveckling
- modell för systemutveckling
- förvaltningsmodell knuten till systemutvecklingsmodellen
- ledning av utvecklingsprojekten
- behörighetskontroll.

Systemägaren är ansvarig för säkerhetsåtgärderna vid utveckling av informationssystemet. Nyutveckling och programunderhåll bör skiljas åt. Vid programunderhåll är det som regel enbart nödvändigt att granska de säkerhetsåtgärder som direkt berörs av de vidtagna åtgärderna. Verifieringen av att informationssystemet uppfyller uppställda säkerhetsmål sker vid systemtesten och i produktionen. Samma

ansvarsförhållanden gäller vid förändring av ett informationssystem som vid anskaffning.

När det gäller källkoden till informationssystem kan en lösning vara att deponera källkoden hos en tredje part om annan överenskommelse inte går att träffa. Av sekretesskäl kan det vara viktigt att reglera åtkomsten till källprogram/-arkiv.

Systemdokumentationen riktas till den som ska underhålla och vidareutveckla informationssystemet och kan lämpligen delas in i en översiktlig och en detaljerad systembeskrivning.

Den översiktliga systembeskrivningen är till för att få en överblick över informationssystemet och förstå systemuppbyggnaden. Den kan t.ex. innehålla:

- en översikt som visar informationssystemets plats i organisationens totala datadrift
- det fysiska och logiska nätets struktur
- vilka delar/moduler systemet/programmet består av
- beskrivning av delarnas uppgift utan detaljer, gärna bilder som visar hur delarna är beroende av varandra
- viktiga datastrukturer, gärna med bilder.

Den detaljerade systembeskrivningen är till för den personal som ska genomföra förändringar eller tillföra nya funktioner. Den kan t.ex. innehålla:

- beskrivning av varje del/modul för sig
- beskrivning av datatyper
- en väl kommenterad programkod.

Delar av systemdokumentationen kan innehålla känsliga uppgifter om informationssystems säkerhetsfunktioner. I vissa fall kan därför åtkomsten till dokumentationen behöva regleras.

Förändring av system i produktion bör konsekvensbedömas vad avser påverkan på säkerhetsfunktioner för sekretess, riktighet och tillgänglighet samt påverkan på gällande kontinuitetsplanering. Samtliga ändringar ska kunna härledas till en ansvarig beställare.

Endast välrenommerade leverantörer bör väljas vid anskaffning av programpaket.

## 12.6 Hantering av teknisk sårbarhet

**Mål:** "Att minska riskerna med utnyttjande av publicerade tekniska sårbarheter."

### Basnivå

- Roller och ansvar ska definieras för hantering av teknisk sårbarhet omfattande
  - övervakning av sårbarheten
  - riskbedömning av sårbarheten
  - programändringar
  - spårning av tillgångar
  - samordningsansvar

# 13. Hantering av informationssäkerhetsincidenter

## 13.1 Rapportering av säkerhetshändelser och svagheter

**Mål:** "Att säkerställa att informationssäkerhetsincidenter och svagheter hos informationssystem rapporteras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid."

**Basnivå**

- Det ska finnas fastlagda rutiner för hur användare ska agera vid funktionsfel, misstanke om intrång eller vid andra störningar (Säkerhetsinstruktion, användare).

En formell rapporteringsrutin bör finnas för hur misstankar om incidenter tas omhand, där kontaktpunkten för inrapportering ska vara känd i hela organisationen.

## 13.2 Hantering av informationssäkerhets-incidenter och förbättringar

**Mål:** "Att säkerställa att ett konsekvent och effektivt angreppssätt tillämpas på hanteringen av informationssäkerhetsincidenter."

**Basnivå**

- Rutiner ska finnas fastlagda för hur uppföljning av funktionsfel, misstanke om intrång eller vid andra störningar (Säkerhetsinstruktion, förvaltning).

Incidenter förekommer i de flesta organisationer. Upphovet till dem kan exempelvis vara interna eller externa intrång och intrångsförsök, felaktig användning av informationssystemen och IT-resurserna o.dyl. Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Regler för hur incidenter följs upp är därför angelägna.

I en process för incidenthantering bör:

- det vara klarlagt hur och till vem rapportering ska ske
- resurser finnas för att prioritera och åtgärda inträffade incidenter
- skeende och åtgärder vara möjliga att följa upp i efterhand
- rutiner finnas för återställning till normal drift efter att en incident åtgärdats

Organisation som på uppdrag ansvarar för drift av informationssystem för annan organisations räkning bör i samarbete med respektive informationssystems systemägare upprätta rutiner för vissa onormala situationer. Rutinerna bör bl.a. ange:

- hur användarna informeras vid driftstörningar.
- hur rapportering ska ske vid störningar, fel och IT-incidenter.
- agerande vid samtidiga störningar i flera system.
- hur prioritering ska göras mellan system.

# 14. Kontinuitetsplanering i verksamheten

## 14.1 Säkerhetsaspekter på kontinuitetsplanering i verksamheten

**Mål:** "Att motverka avbrott i organisationens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer och att säkra återstart inom rimlig tid."

### Basnivå

- Systemägaren ska besluta om den längsta tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras.
- Det ska finnas en dokumenterad avbrottsplan som omfattar de återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie drift för att informationssystemen ska kunna återstartas inom fastställd tid.
- Återstartsrutiner ska:
  - finnas för informationssystem
  - dokumenteras (Säkerhetsinstruktion, kontinuitet och drift).
- Befintliga reservrutiner ska dokumenteras (Säkerhetsinstruktion, kontinuitet och drift).
- Det ska finnas en dokumenterad gemensam avbrottsplan för IT-verksamheten som är avstämd mot de enskilda informationssystemens avbrottsplaner.
- Det ska finnas en dokumenterad rutin för att informera om avbrott och återställningsarbete som
  - är kommunicerad och testad.
  - inbegriper alla som, direkt eller indirekt, är beroende av informationssystemet och dess information.
- Omständigheter som ska betecknas som katastrof för verksamheten ska klarläggas.

För kontinuitetsplaneringen ska kritiska verksamhetsprocesser identifieras. Säkerhetskraven på kontinuitet i verksamheten ska integreras med andra kontinuitetskrav på drift, personalbemanning, material, transport och resurser. Informationssäkerhet bör vara en integrerad del av den gemensamma processen för kontinuitetsplanering inom organisationen.

Kontinuitetsplaneringen bör innefatta åtgärder för att identifiera och minska risker, begränsa konsekvenserna av skadliga incidenter och säkerställa att den information som krävs för verksamheten är tillgänglig och riktig.

Kontinuitetsplaneringen är en process som bl.a. innebär att ta fram en avbrottsplan och en katastrofplan.

Avbrottsplaneringen måste anpassas till informationssystemens vikt för verksamheten och vara en integrerad del i det totala säkerhetsarbetet för verksamheten. Informationssystemen behöver ges en prioritetsordning. Avbrottsplaneringen utgår från att återstart ska kunna ske så att kraven på tillgänglighetskrav uppfylls för respektive informationssystem. Avbrottsplanen ska beskriva de åtgärder som ska säkerställa fortsatt verksamhet vid störning eller avbrott i IT-driften inom en viss tid och redovisa de reserv- och återstartsrutiner för IT-driften som krävs för detta. Ett stort antal åtgärder kan därvid vara aktuella och avse områden som dokumentation, bemanning, brand, skydd mot skadlig programkod, elförsörjning samt säkerhetskopiering och förvaring av datamedia.

Det är också viktigt att reglera ansvarsförhållanden vid avbrottssituationer, exempelvis ansvaret för de åtgärder som krävs för att hantera den uppkomna situationen.

Organisationens ledning ska överväga om det finns särskilda skäl att upprätta en katastrofplan. Utgångspunkten för en katastrofplan är verksamhetsledningens bedömning av vilka omständigheter som skulle kunna medföra konsekvenser som betecknas som katastrofala för verksamheten. Katastrofplanering är en process som till stor del måste ledas och inriktas av verksamhetsledningen och har som mål att skapa förutsättningar för att upprätta en katastrofledning som operativt ska kunna leda verksamheten.

# 15. Efterlevnad

## 15.1 Efterlevnad av rättsliga krav

**Mål:** "Att undvika handlande i strid med författningar eller avtalsförpliktelser och andra säkerhetskrav."

**Basnivå**

- Programvaror ska endast användas i enlighet med gällande avtal och licensregler.
- För efterlevnad av upphovsregler ska det finnas regler för godkännande och distribution av program som används i verksamheten.
- För informationssystem som hanterar allmän handling ska
  - gallringsbeslut finnas
  - arkivering och gallring ske i enlighet med gallringsbeslut.
- Rutin för utlämnande av information från informationssystem ska finnas för system som hanterar allmän handling.
- Licens eller annat avtal om nyttjanderätt ska finnas för alla ingående program och programkomponenter som ingår i informationssystem och där organisationen inte har äganderätt.
- Licens ska revideras årligen och avse rätt antal användare, rätt dator etc.
- Anvisning för skydd av organisationens register och handlingar för att efterleva gällande lagstiftning ska dokumenteras (Säkerhetsinstruktion, förvaltning) och omfatta:
  - identifieringsprinciper för dokument
  - bevarande, lagring, hantering och kassation
  - tidskrav på förvaring etc.
  - särskilda behov av skydd från förlust, förstörelse och förvanskning.
- Informationssystem som hanterar personuppgifter ska vara förtecknat och anmält till personuppgiftsombud (om sådant utsetts).

- Bearbetning av personuppgifter samt information om respektive samtycke till bearbetningen ska ske i enlighet med vad som överenskommits med personuppgiftsombud eller i enlighet med PUL.

Bestämmelser av särskild vikt avseende krav på vidtagna skyddsåtgärder är:

- Personuppgiftslagen
- Offentlighet och sekretesslagstiftning
- Upphovsrättslagen
- Patentlagen
- Arkivlagen och arkivförordningen och gällande gallringsföreskrifter
- Säkerhetsskyddslagen
- Särskild myndighetslagstiftning med inriktning på informationsbehandling (Socialförsäkringsregisterlag, patientjournallag etc.)
- Bokföringsförordningen

Tryckfrihetsförordningens krav på att allmän handling ska vara tillgänglig ska tillgodoses.

**Tips!**
Viss vägledning för tillämpning av offentlighets- och arkivlagstiftning ges i Statskontorets publikation "Offentlighet och IT 2002:1".

## 15.2 Efterlevnad av säkerhetspolicies, -standarder och teknisk efterlevnad

**Mål:** "Att säkerställa att system följer organisationens säkerhetspolicies och -standarder."

**Basnivå**

- Interna och externa penetrationstester ska göras återkommande.
- Ledningspersoner ska regelbundet granska att säkerhetsrutiner, -policy och -normer efterlevs.
- Penetrationstester på externa kommunikationssystem (FW etc.) respektive på interna informationssystem ska göras återkommande.

## 15.3 Att beakta vid revision av informationssystem

**Mål**: "Att maximera revisionens effektivitet och samtidigt minimera driftstörningar orsakade av revisionen."

### Basnivå

- Åtgärder för kontroller av system i drift måste planeras för att minimera risken för störningar
- Åtkomst till revisionshjälpmedel ska begränsas.

## KBM REKOMMENDERAR

2006:1 Basnivå för informationssäkerhet (BITS)
Utgåva 3

2004:1 Kommunens plan för hantering av extraordinära händelser
Vägledning från Krisberedskapsmyndigheten

2003:2 Basnivå för IT-säkerhet (BITS)

2003:1 Risk- och sårbarhetsanalyser
Vägledning för statliga myndigheter

## SEMA RECOMMENDS

2003:2 Basic level for IT Security (BITS)

ISSN: 1652-2893
ISBN: 91-85053-97-x

**Krisberedskapsmyndigheten**

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se