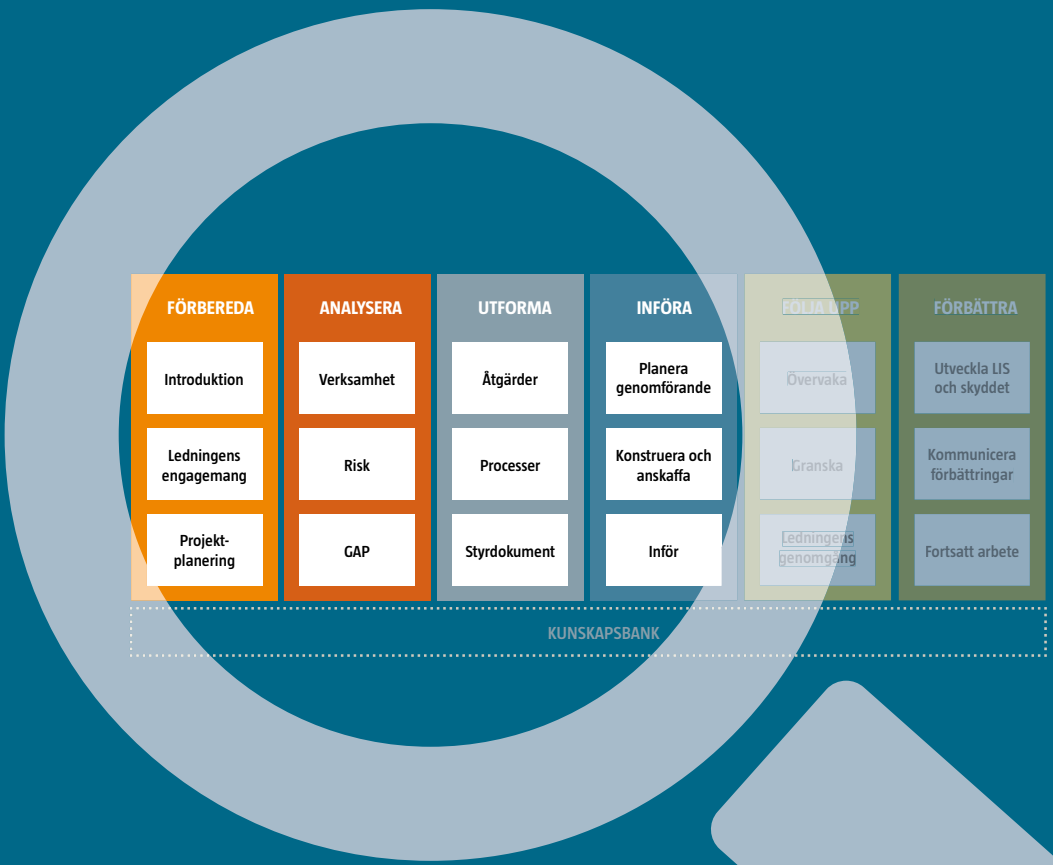
Myndigheten för samhällsskydd och beredskap

# Kommunens informationssäkerhet

## – en vägledning



# Kommunens informationssäkerhet

– en vägledning

Kommunens informationssäkerhet – en vägledning

Utgiven av:
Myndigheten för samhällsskydd och beredskap (MSB)

Vid frågor kontakta:
Enheten för samhällets informationssäkerhet, MSB

Layout: Advant Produktionsbyrå AB
Tryck: DanagårdLiTHO

Publikationsnummer: MSB508 - december 2012
ISBN: 978-91-7383-304-2

# Innehållsförteckning

# Förord

Sveriges kommuner hanterar en betydande del av samhällets tjänster och kommunernas informationsförsörjning är därför en kritisk del i samhällets informationssäkerhet. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en kommuns olika förvaltningar och bolag är det av stor betydelse att informationssäkerhetsarbetet bedrivs metodiskt och långsiktigt. Syftet med denna vägledning är att på ett konkret sätt stödja kommuner att bedriva ett sådant arbete.

Myndigheten för samhällsskydd och beredskap (MSB) har givit ut föreskrifter om statliga myndigheters informationssäkerhet. Föreskrifterna pekar på att myndigheterna ska följa de internationella standarderna på området, ISO/IEC 27001 och ISO/IEC 27002. Dessa föreskrifter är endast bindande för statliga myndigheter men det finns stora vinster med att också kommuner arbetar med informationssäkerhet på samma systematiska sätt. Utvecklingen inom e-förvaltning kommer att kräva att kommuner, myndigheter och landsting samverkar än mer. Om alla parter arbetar efter gällande standarder på området kommer det att finnas en ömsesidig förståelse vad gäller säkerhetsfrågor och ett gemensamt språk kring detta. Det skapar exempelvis ökad effektivitet, högre säkerhetsmedvetande och minskade kostnader.

På www.informationssäkerhet.se finns ett metodstöd för organisationer som ska införa eller förbättra sitt ledningssystem för informationssäkerhet med utgångspunkt i standarderna. Den här vägledningen presenterar metodstödet på en övergripande nivå och med kommunernas verksamhet och förutsättningar i fokus.

Denna vägledning riktar sig främst till den som praktiskt ska bedriva arbetet med kommunens informationssäkerhet. Det bör dock betonas att det är viktigt att engagera representanter från i princip hela organisationen i det systematiska informationssäkerhetsarbetet. Denna vägledning är en första utgåva och kommer att uppdateras regelbundet.

**Richard Oehme, Enhetschef**
Enheten för samhällets informationssäkerhet

# 1. Inledning

## 1.1 Syfte

Informationssäkerhet handlar om att ge kommunens information rätt skydd och omfattar:

- **Tillgänglighet:** Att information är tillgänglig i förväntad utsträckning och inom önskad tid
- **Riktighet:** Att den skyddas mot oönskad och obehörig förändring eller förstörelse
- **Konfidentialitet:** Att den inte i strid med lagkrav eller lokala överenskommelser/riktlinjer tillgängliggörs eller delges obehörig
- **Spårbarhet:** Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)

Informationssäkerhet omfattar *hela kommunens verksamhet och all information* oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system så handlar informationssäkerhet även om teknik.

För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en kommuns olika förvaltningar och bolag är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt. Myndigheten för samhällsskydd och beredskap (MSB) har därför, i samarbete med andra organisationer och med utgångspunkt i de internationella standarderna i ISO/IEC 27000-serien, tagit fram ett metodstöd för ett sådant systematiskt arbete. Metodstödet återfinns i sin helhet på webbadressen www.informationssäkerhet.se.

Den här vägledningen presenterar metodstödet på en övergripande nivå och med kommunernas speciella verksamhet och förutsättningar som utgångspunkt. Vägledningen visar hur kommunen på ett relativt enkelt sätt kan få en god styrning av informationssäkerheten.

Kommunen kan välja att följa vägledningen i sin helhet eller bara valda delar. Oavsett vilket så måste insatserna anpassas till den egna organisationens specifika situation.

## 1.2 Målgrupp

Vägledningen riktar sig främst till den som praktiskt ska bedriva arbetet med att etablera styrning över informationssäkerheten inom en kommun eller någon av dess förvaltningar eller bolag. Det gäller främst verksamhetschefer, säkerhetschefer och informationssäkerhetsansvariga. Det bör dock betonas att i arbetet med att införa eller vidareutveckla kommunens informationssäkerhet är det viktigt att engagera representanter från i princip hela kommunen i arbetet. Exempelvis behövs kunskap om verksamhetens behov, IT-miljön, rättsliga aspekter, ekonomi och revision.

## 1.3 Nytta

Systematiskt och långsiktigt arbete med informationssäkerhet i enlighet med denna vägdelning och metodstödet ger följande nytta för kommunen:

- **Ekonomi:** Kommunen får en god informationssäkerhet som är anpassad efter verksamhetens förutsättningar och behov. Kommunen får en bra säkerhetsekonomi genom att säkerhetsincidenter kan undvikas via ett väl avpassat, ändamålsenligt och kostnadseffektivt skydd.
- **Förtroende:** Genom säkerhet i informationshanteringen kan omvärlden och invånarnas förtroende för kommunen bibehållas och öka.
- **Efterlevnad:** Kommunen säkerställer att legala krav efterlevs och revisioner klaras bättre. Det kan gälla exempelvis skydd av personuppgifter i enlighet med personuppgiftslagen och krav på internkontroll.
- **Styrning:** Kommunledningen får möjlighet att styra och följa upp informationssäkerheten så att man kan bevaka att skyddet är effektivt och ändamålsenligt.
- **Kommunikation:** Kommunen ansluter sig till ett vedertaget sätt att arbeta med informationssäkerhet och anammar en gemensam terminologi. Därigenom blir det lättare, och ofta en förutsättning för, att kommunicera och samarbeta om gemensamma informationssäkerhetsfrågor med kollegor i andra kommuner och organisationer då det handlar om tillit.

## 1.4 Ledningssystem

Genom att använda den här vägledningen och metodstödet etableras ett *"ledningssystem för informationssäkerhet"* (LIS) som genom en policy och andra styrande dokument huvudsakligen anger hur informationssäkerheten är organiserad, vem som ansvarar för att göra vad och när, samt hur informationssäkerhetsfrågor ska rapporteras till kommunens ledning.

Sättet att styra och leda informationssäkerheten i kommunen måste ligga i linje med kommunens sätt att i övrigt styra och leda verksamheterna.

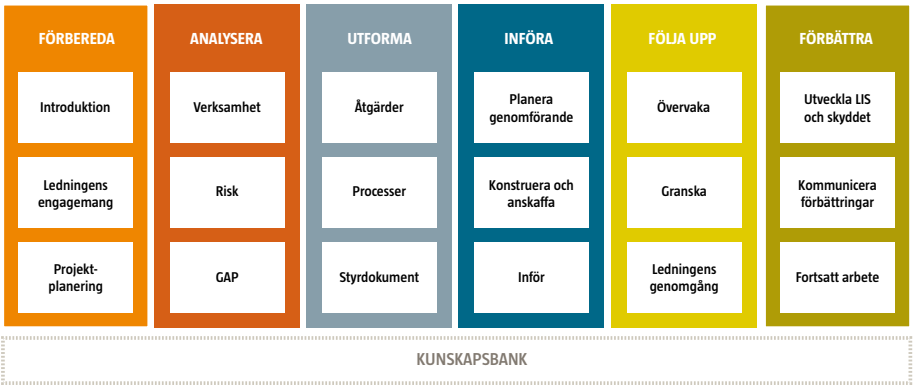
Ett etablerat LIS kan på kommunens begäran granskas av ett oberoende organ som därefter utfärdar ett certifikat, vilket intygar att kommunens ledningssystem lever upp till kraven i ISO/IEC 27001.

## 1.5 Vägledningen

Det metodstöd som finns på webbplatsen www.informationssäkerhet.se är utformat för att passa alla typer av organisationer och behandlar därför frågan på ett mer generellt sätt. Denna vägledning, vilken specifikt riktar sig till kommuner, bygger på erfarenheter och resultat från MSB:s samarbete med några kommuner som använt metodstödet för att etablera en styrning av sin informationssäkerhet. Genom att gå igenom vägledningen får den som har fått i uppdrag att leda eller samordna kommunens informationssäkerhetsarbete:

- **Överblick:** En samlad överblick av vad ett ledningssystem är och en beskrivning steg för steg vad arbetet att införa ett sådant system innebär.
- **Praktiska exempel**: Baserat på praktiskt arbete som genomförts i ett antal kommuner.
- **Mallar:** Länkar till mallar och andra stöddokument.
- **Metodstöd:** Länkar till metodstödet på www.informationssäkerhet.se där det finns mer ingående beskrivningar av metodens olika steg.

Figuren nedan ger en överblick över de steg kommunen behöver gå igenom för att etablera styrning över sin informationssäkerhet.




*Figur: Överblick över metodstödet på www.informationssäkerhet.se*

Varje aktivitet som ingår i de tre delprocesserna *analysera*, *utforma* och *införa* i figuren beskrivs i ett eget avsnitt i denna vägledning. Varje sådant avsnitt innehåller en beskrivning av aktiviteten, en att-göra-lista, aktivitetens resultat samt var man kan erhålla ytterligare stöd, exempelvis i form av mer information, mallar och praktiska kommunrelaterade exempel. Viktiga förutsättningar tas även upp (*förbereda*), men inte den löpande förvaltningen som tar vid efter det att ledningssystemet är etablerat (*följa upp* och *förbättra*).

Denna skrift kommer successivt att omarbetas i enlighet med kommunernas återkoppling. Den senaste versionen hittar du alltid på www.informationssäkerhet.se.

# 2. Kommuners informationssäkerhetsarbete

## 2.1 Förutsättningar och behov

Förutsättningarna för informationssäkerhetsarbete inom en kommun liknar till många delar vilken annan organisation som helst, men det finns också väsentliga skillnader. De egenskaper kommuners verksamhet har ger viktiga ingångsvärden för utformningen av informationssäkerhetsarbetet. Några sådana egenskaper är exempelvis:

- **Bredd i verksamheten**
  – En kommuns verksamhet bedrivs inom vitt skilda områden och utgör merparten av den offentliga samhällsservicen till medborgarna.
- **Självstyrande förvaltningar**
  – Den verksamhet som bedrivs är spridd på olika förvaltningar och kommunägda företag som till olika grader är självstyrande.
- **Samhällsviktiga funktioner**
  – Viktiga funktioner i samhället som exempelvis vård, skolor, vatten och värme ligger oftast inom ramen för verksamheten. Störningar i dessa funktioner kan medföra allvarliga konsekvenser.

Det finns således många likheter, men även olikheter mellan kommunerna. Det gäller exempelvis tillgängliga resurser. I en undersökning som MSB genomförde under 2012 konstaterades att flertalet av kommunernas informationssäkerhetssamordnare ägnade mindre än 25 % av sin arbetstid åt dessa frågor. Mindre kommuner, med begränsade resurser, väljer dock ofta att samarbeta med andra kommuner kring informationssäkerhetsarbetet, vilket kan ge fördelar på flera plan.

Behovet av informationssäkerhet har ökat i takt med att kommuninvånarna förväntar sig snabbare kommunikation med kommunerna, dels via självbetjäning med hjälp av olika e-tjänster, och dels i sin direktkommunikation med kommunen. Invånarna förväntar sig att kommunen ska hantera information som rör dem, exempelvis personuppgifter och information om de olika tjänster de använder, på ett säkert sätt. I samband med kriser krävs också effektiv och säker kommunikation med berörda verksamheter och invånare. Allt detta ställer krav på kommunens organisation och arbetet med informationssäkerhet.

## 2.2 Informationssäkerhetssamordning inom kommunen

Många kommuner har en medarbetare med ett utpekat ansvar för informationssäkerheten, exempelvis en IT-strateg, informationssäkerhetschef eller informationssäkerhetssamordnare. Undersökningar har visat att utgångspunkterna för dennas arbete ofta kan beskrivas på följande sätt:

- **Ansvarets placering**
  – Kommunens IT-avdelning eller säkerhetsfunktion är typiska placeringar för samordningsansvaret för kommunens informationssäkerhet.
- **Deltid med informationssäkerhet**
  – Samordnaren av informationssäkerheten har ofta detta som *en* av sina arbetsuppgifter vid sidan av annat. Det gör att många kommuner saknar någon som arbetar heltid med just informationssäkerhet.
- **Behov av stöd**
  – Den som har fått ett sådant samordningsansvar är ofta i behov av utbildning och stöd för att effektivt kunna utföra sina uppgifter.

Det bör i kommunen finnas en tjänst med utpekat ansvar för informationssäkerheten. Det är även centralt att denna person har god kunskap om informationssäkerhet och får tillräcklig tid och resurser för att utföra sitt arbete. Erfarenheter visar att de organisationer som har detta på plats får en bättre kontroll över risker och organisationens skydd vilket i förlängningen leder till minskade risker, att omvärldens förtroende för organisationen ökar och oväntade kostnader kan förhindras. Informationssäkerhet handlar om hela kommunen som organisation och denna tjänst bör därför organisatoriskt placeras så att samarbete med och stöd från bland annat jurister, HR, kommunikation och IT kan bedrivas på bästa sätt.

## 2.3 Ledningens engagemang

All erfarenhet visar att ledningens engagemang är kritiskt för att informationssäkerhetsarbetet ska kunna bli effektivt och ändamålsenligt. Bristande informationssäkerhet märks först när en incident inträffar, vilket gör att frågan ofta får stå tillbaks till förmån för sådant som är mer påtagligt. Att inte ta informationssäkerheten på allvar kan medföra negativa konsekvenser för kommunens verksamhet och ekonomi, samt drabba invånarna. Det är därför viktigt att kommunens ledning kan se såväl vinsterna med ett systematiskt informationssäkerhetsarbete som vilka risker det finns med avsaknaden av det. Ledningens roll kan beskrivas som följer:

- **Ledningen har ansvaret**
  – Ledningen har det övergripande ansvaret för informationssäkerheten inom kommunen och är ytterst ansvarig vid incidenter. Alla kommunala nämnder har också ett ansvar för att följa personuppgiftslagen och behandla personuppgifter på ett korrekt sätt.
- **Engagemang skapar medvetenhet**
  – En ledning som är engagerad och införstådd med verksamhetsnyttan med ett systematiskt informationssäkerhetsarbete skapar förutsättningar för en hög säkerhetsmedvetenhet i hela kommunen.
- **Positiv kommunikation**
  – Det är viktigt att ledningen kommunicerar ut att informationssäkerhetsarbetet är till allas fördel och att det skapar bättre förutsättningar för det vardagliga arbetet.
- **Mandat för samordningsansvaret**
  – Kommunens ledning måste kommunicera till de olika förvaltningarna och bolagen som berörs att ett samordningsansvar utpekats och att den medarbetaren har mandatet att arbeta med informationssäkerhetsfrågorna ute i verksamheten.

En aktiv ledning som tar initiativ i informationssäkerhetsfrågan och tydliggör ansvaret, skapar goda förutsättningar för att styrningen av kommunens informationssäkerhet blir effektiv. Ledningen bör också minst årligen följa upp och utvärdera informationssäkerhetsarbetet och besluta om dess framtida inriktning.

## 2.4 Lagar och förordningar

Lagar och förordningar ställer krav på kommuners informationssäkerhet. Följande lagar och förordningar ställer direkt eller indirekt krav på informationssäkerheten (exempel):

- *Personuppgiftslagen*
- *Offentlighets- och sekretesslagen*
- *Säkerhetsskyddslagen*
- *Arkivlagen*
- *Patientdatalagen*
- *Förvaltningslagen*
- *Lag om offentlig upphandling*
- *Lag om kommunal redovisning*

- *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*
- *Kommunallagen*

För hälso- och sjukvårdsverksamheten inom en kommun gäller även att följa de krav som ställs på informationssäkerheten enligt Socialstyrelsens föreskrifter (SOSFS 2008:14). Kraven omfattar hur patientuppgifter ska hanteras samt hur informationssäkerhetsarbetet ska bedrivas och vad det ska omfatta.

I och med att det finns många olika verksamheter inom en kommun är det också många olika legala krav att förhålla sig till. På www.informationssäkerhet.se finns en sammanställning av de olika lagar och förordningar en kommun har att förhålla sig till med bäring på informationssäkerhet. Genom att utforma sin styrning av informationssäkerheten i enlighet med denna handbok tar kommunen viktiga steg till att uppfylla de lagkrav som gäller.

## 2.5 Relevant bakgrundsmaterial

Många kommuner har arbetat med Krisberedskapsmyndighetens rekommendationer och verktyg BITS och BITS Plus (BITS står för Basnivå för Informationssäkerhet). MSB lyfter nu istället fram de internationella standarderna i ISO/IEC 27000-serien och metodstödet på www.informationssäkerhet.se. De tidigare insatserna enligt BITS kan användas som en utgångspunkt i det vidare arbetet, exempelvis vad avser utformning av skydd för specifika informationssystem, tidigare inventering av kritiska informationstillgångar samt redan framtagna styrande dokument som informationssäkerhetspolicy. Tidigare insatser och erfarenheter inom informationssäkerhet, oavsett metod, bör utgöra en av utgångspunkterna när kommunen följer denna handbok.

## 2.6 Risk- och sårbarhetsanalyser

Samtliga Sveriges kommuner är skyldiga att genomföra risk- och sårbarhetsanalyser (RSA) enligt lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH). Oavsett var i landet en kris inträffar får den alltid konsekvenser i en eller flera kommuner. Då gäller det att i förväg ha analyserat risker, sårbarheter, sin egen förmåga och sina samverkansbehov. MSB har i en föreskrift förtydligat vad som ska ingå i en RSA. Bland de olika förhållandena som kommunen ska kunna redogöra för finns även krav på rapportering av hur god förmåga kommunen har att skydda informationens konfidentialitet, tillgänglighet och riktighet.


Forskning för
samhällsskydd
och beredskap

# 3. Förberedelser för införande av ett LIS

## 3.1 Projekthantering

**Organisera arbetet som ett projekt**
Erfarenheten visar att det är en stor fördel att organisera arbete med att etablera styrning över kommunens informationssäkerhet i form av ett projekt. I det fall kommunen har en fastställd projektstyrningsmetod blir det naturligt att även det här projektet följer den metoden. Projektet beskrivs i en projektplan som kan ange förväntad nytta, målsättning, tilldelade resurser, bemanning, övergripande planering samt plan för kommunikation för förankring. Innan projektet startar bör planen vara fastställd och beslutad.

**Definiera omfattningen**
Det går att definiera omfattningen för ett ledningssystem för informationssäkerhet så att det omfattar hela organisationen eller delar av den, exempelvis en viss förvaltning eller ett område. Om ledningen väljer att exkludera vissa delar av organisationen från omfattningen av ledningssystemet bör motivet till detta dokumenteras.

**Avgränsa projektet tydligt**
Erfarenheten visar att projekten kan fastna i detaljer. Det gäller därför att hålla fast vid den fastställda projektplanen. Nya uppdrag, behov av åtgärder, analyser etc. som inte finns i projektplanen antecknas för att tas om hand i ett senare skede. Saker som kräver akuta åtgärder bör så långt som möjligt överlämnas till linjeverksamheten, det vill säga utanför projektet, för att åtgärdas där.

**Identifiera andra pågående projekt**
Andra relaterade pågående projekt och insatser bör inventeras så att projektet kan etablera samordning med dessa. Det kan gälla exempelvis framtagande av ny IT-strategi eller generell säkerhetspolicy.

**Identifiera och kontakta berörda**
Vissa aktiviteter, inte minst under analysskedet, bör involvera personer från de olika verksamheterna. Det kan handla om verksamhetschefer, IT-personal, jurister, systemförvaltare med flera. Då är det viktigt att tidigt identifiera och kontakta berörda så att de kan reservera tid för sin insats.

**Projektsponsor från ledningen**
För att projektet inte ska stanna upp är det viktigt att ledningen kontinuerligt följer arbetet. Projektledaren bör också löpande få möjlighet att redovisa hur arbetet fortskrider för ledningen.

**Identifiera och mät nyttan**
Det är viktigt att identifiera och kommunicera den nytta som ett införande av ett ledningssystem för informationssäkerhet ger kommunen. När projektets effektmål formuleras bör man sträva efter att göra dessa så mätbara som möjligt.

## 3.2 Bemanning

Projektplanen bör inrymma en beskrivning av vilken kompetens projektet bemannas med. Typiska roller i ett projekt för att etablera styrning över kommunens informationssäkerhet:

**Projektsponsor/uppdragsgivare:**
Exempelvis Kommunfullmäktige, Kommunchef eller Förvaltningschef.
*Ansvar*:

- uppdragsgivare och huvudansvarig för projektet
- fastställer projektplanen
- tillhandahåller ekonomiska resurser
- beslutar när projektet är slutfört

**Projektstyrgrupp:**
Personer som ledningen tillsatt för att styra projektet mot uppsatta mål.
*Ansvar*:

- följer projektarbetet och tar ställning till delleveranser
- beslutar godkännande av det som projektet levererar
- tar ställning till avvikelser från projektplanen

**Projektledare:**
Exempelvis informationssäkerhetschef eller -samordnare.
*Ansvar*:

- ansvarar för att projektet genomförs enligt plan
- ansvarar för projektledning
- kontinuerlig rapportering/uppföljning till uppdragsgivaren och till referensgruppen

- tydliggör problemställningar och eventuella avvikelser
- ansvarar för att uppdraget levereras

**Projektgrupp:**
Representanter från exempelvis personalavdelning, IT-avdelning, rättsavdelning, representanter från olika verksamheter.
*Ansvar*:

- tillsammans med projektledaren ansvarar de för att projektet genomförs enligt plan
- förankra de lösningar som tas fram i organisationen

**Kommunikationsansvarig:**
Person med god kommunikativ förmåga.
*Ansvar*:

- tar fram kommunikationsplan och initierar revideringar vid behov
- ansvarar för att föreslagna kommunikationsaktiviteter genomförs och följs upp

**Ordinarie verksamhet:**
I samband med att man bemannar projektet kan det vara värt att komma ihåg att följande roller som ofta redan finns påverkas av och påverkar informationssäkerheten på kommunen:

- personuppgiftsombud
- arkivarie
- säkerhetschef eller -samordnare
- kommunjurist
- IT-chef
- miljösamordnare
- kvalitetsansvarig
- utvecklingschef

## 3.3 Checklista förberedelser

Innan det är dags för de första analyserna, kontrollera att följande är gjort:

- Ledningen är informerad och engagerad i informationssäkerhetsarbetet
- Fastställd och av ledningen beslutad projektplan finns
- Resurser som kommer krävas är beskrivna och tilldelade
- Ansvarig för projektets genomförande är utsedd och har ett av ledningen uttalat mandat
- Ledningen har tydliggjort för berörda verksamheter hur projektet ska prioriteras och vilka resurser som kan tas i anspråk
- Denna vägledning är genomläst
- Kunskap om metodstödet på www.informationssäkerhet.se finns

I nästa avsnitt presenteras de olika stegen i informationssäkerhetsarbetet och i enlighet med metodstödet inleds arbetet med *verksamhetsanalysen.*


Larsåke Larsson
med e-förvaltning

# 4. Analysera

## 4.1 Verksamhetsanalys

### Beskrivning

*Verksamhetsanalysen* hjälper kommunen att identifiera de viktigaste informationstillgångarna, ex. IT-system. Som stöd finns en lista över vanligen förekommande informationstillgångar i kommunal verksamhet som kan vara bra att utgå ifrån (se Bilaga 2: *Informationstillgångar*). Den kan behöva kompletteras ytterligare och då kan det vara bra att ta upp frågan med respektive förvaltningschef eller motsvarande. När man väl vet vad som ska skyddas identifieras vilka krav som ställs på respektive tillgång. Det gäller kommunens egna säkerhetskrav för tillgångarna eller krav som kommer utifrån i form av exempelvis avtal och lagar. Det är verksamheternas processer som till stor del avgör både vilka informationstillgångar som är viktiga samt vilka kraven är.

Dessa tillgångar klassificeras sedan. *Varje* informationstillgång analyseras mot de identifierade kraven (både de interna och de externa) för att se vilken konsekvensen förväntas bli vid förlust av konfidentialitet, riktighet, tillgänglighet och spårbarhet. Denna *klassning* av informationstillgångar ska inte förväxlas med *klassificering* av dokument och filer, vilket ofta är kopplat till hanteringsregler för hur en viss typ av dokument får hanteras.

### Att göra

1. Identifiera informationstillgångar (ett tips är att be respektive förvaltningschef/sektorchef samla in de mest kritiska informationstillgångarna inom sin verksamhet)
2. Identifiera legala krav
3. Identifiera verksamhetens krav
4. Ta klassningsbeslut

### Resultat

Resultatet av verksamhetsanalysen är en strukturerad förteckning över informationstillgångarna där också verksamhetens och legala säkerhetskrav dokumenterats. I förteckningen är varje informationstillgång klassificerad utifrån *konfidentialitet*, *riktighet*, *tillgänglighet* och *spårbarhet*.

### Stöd

1. Mall: Analys av informationstillgång – Mall MSB.
2. Beskrivning: Verksamhetsanalys – Metodstöd MSB, www.informationssäkerhet.se

## 4.2 Riskanalys

### Beskrivning

Med kunskap om informationstillgångar och verksamhetens krav från verksamhetsanalysen innan, genomförs en riskanalys för att identifiera och senare hantera de risker som kan påverka verksamhetens informationssäkerhet. Riskernas sannolikhet och konsekvens bedöms av nyckelpersoner från verksamheten. Huvudresultatet av en riskanalys är en förteckning över risker, deras potentiella skadeverkning, och tänkbara sätt att hantera riskerna på. Utöver detta genererar själva arbetsprocessen ytterligare ett antal positiva bieffekter.

Till exempel:

- Vi lär oss hantera risker
- Vi får fram en realistisk bild av verkligheten
- Vi blir medvetna om hoten
- Vi gör en realistisk och trovärdig värdering av riskerna
- Vi tar fram beslutsunderlag för att kunna fatta rätt beslut

Riskanalyser för informationssäkerhet kan göras i många olika situationer och på många olika nivåer – för verksamheten som helhet, för en särskild informationstillgång, för en specifik applikation, för en serverhall, för en verksamhetsprocess och så vidare.

### Att göra

1. Välj och beskriv informationstillgångar som ska analyseras
2. Identifiera hot mot informationstillgångarna
3. Sammanställ och gruppera hot
4. Bedöm risk (konsekvens och sannolikhet)
5. Ta fram åtgärdsförslag

### Resultat

Riskanalysens resultat är att hot mot informationstillgångar bedömts i ljuset av verksamhetens krav (från verksamhetsanalysen). Tillsammans med aktiviteten verksamhetsanalys har nu riskanalysen definierat verksamhetens skyddsbehov – vi vet vad som ska skyddas, varför, och mot vad.

### Stöd

1. Mall: Analys av informationstillgång – Mall MSB.
2. Beskrivning: Riskanalys – Metodstöd MSB, www.informationssäkerhet.se

## 4.3 GAP-analys

### Beskrivning

Från verksamhetsanalysen och riskanalysen är nu behoven, kraven och riskerna kartlagda vilket ger en bild av verksamhetens skyddsbehov. Med detta som utgångspunkt jämförs det existerande skyddet med de säkerhetsåtgärder som föreslås i standarden ISO/IEC 27001. Med GAP-analys menas därför gapet mellan det som standarden beskrivs som best practice (en lista med krav eller säkerhetsåtgärder) och den säkerhetsnivå som råder i verksamheten.

Syftet med aktiviteten är att ge:

- Bekräftelse på att skyddet är infört i tillräcklig omfattning
- En uppfattning om kvalitén på säkerhetsarbetet
- Information om styrkor och svagheter i skyddet
- Ett underlag att gå vidare med i införandet av ledningssystemet

### Att göra

1. Identifiera kunskapskällor (ex. personer och dokument)
2. Dokumentera nuläget
3. Dokumentera förbättringsåtgärder

### Resultat

Resultatet av GAP-analysen är en beskrivning av verksamhetens faktiska informationssäkerhetsnivå genom en inventering av existerande säkerhetsåtgärder. Analysen ger ”gapet” mellan vad som krävs (skyddsbehovet) och nuläget.

### Stöd

1. Lista på säkerhetsåtgärder från ISO/IEC 27001 (se Bilaga 3)
2. Mall: Gap-analys – Mall MSB
   www.informationssäkerhet.se
3. Beskrivning: GAP-analys – Metodstöd MSB, www.informationssäkerhet.se

Gapanalysen var sista aktiviteten i processteget ”Grundläggande analys” och nu har organisationen en bra dokumentation över alla informationstillgångar, risker och sårbarheter. Med denna kunskap går det att utforma ett lämpligt sätt att styra och leda ledningssystemet för informationssäkerhet.

# 5. Utforma

## 5.1 Välj säkerhetsåtgärder

### Beskrivning

Med utgångspunkt i skyddsbehovet fastställs de mål och säkerhetsåtgärder som krävs för en balanserad informationssäkerhet. Grunden är listan på åtgärder i standarden ISO/IEC 27001 (se Bilaga 3: Säkerhetsåtgärder), vilken kompletteras vid behov. Införandet av en säkerhetsåtgärd är något man gör för att minska de risker man tidigare identifierat.

Valet av säkerhetsåtgärder beror på överväganden såsom; 1) behovet av skydd, 2) åtgärdens kostnad, 3) dess förväntade effekt, 4) alternativa investeringar. I det här läget prioriteras inte åtgärderna – här gäller det endast ifall man väljer att ha med dem eller inte.

Både Riskanalysen och GAP-analysen indikerar potentiella säkerhetsåtgärder som verksamheten kan välja att införa.

En bra utgångspunkt är att börja med att titta på de säkerhetsåtgärder som GAP-analysen efterfrågade, och som följer 27002 (best practice):

- Vilka av dessa åtgärder finns på plats hos oss?
- Givet resultatet i tidigare analyser – vilka åtgärder bör finnas på plats?

### Att göra

1. Ta del av kunskap från Verksamhetsanalys, Riskanalys och GAP-analys
2. Välj säkerhetsåtgärder (beroende på behov, kostnad och effekt)
3. Dokumentera valet av säkerhetsåtgärder

### Resultat

Resultatet är en lista på valda säkerhetsåtgärder. För varje vald åtgärd beskrivs namn på åtgärden, vem som är ansvarig och motiv till valet.

### Stöd

1. Beskrivning: Fastställ säkerhetsåtgärder – Metodstöd MSB, www.informationssäkerhet.se

## 5.2 Utforma säkerhetsprocesser

### Beskrivning

Från föregående aktivitet finns beslutade säkerhetsåtgärder. Dessa kan vara av teknisk eller administrativ karaktär. En del av de beslutade säkerhetsåtgärderna består av, eller är beroende av, processer som måste finnas på plats. Med process avses en samling i förväg uttänkta, länkade och dokumenterade aktiviteter som svarar mot ett fastställt behov inom informationssäkerhetsarbetet. Exempel på processer kan vara incidenthantering, behörighetsadministration och patchhantering, men även den generella processen för att styra och leda informationssäkerhetsarbetet.

Syftet med att utforma säkerhetsprocesserna är att identifiera och kartlägga de säkerhetsprocesser som är nödvändiga för att upprätthålla en tillfredställande informationssäkerhet enligt uppställda krav och mål i verksamheten.

Planeringen för detta arbete går ut främst på att sätta ihop arbetsgrupperna som ska jobba med identifieringen och framtagandet av säkerhetsprocesserna. Det är betydelsefullt att arbetsgruppen består av en bred kompetens och representerar hela organisationen.

Utformningen av processerna består i huvudsak att besvara frågorna; vad, varför, vem, var, när och hur. Arbetsformen vid processframtagandet kan bestå av arbetsmöten i form av s.k. workshops.

### Att göra

1. Identifiera vilka säkerhetsåtgärder som kräver processer
2. Dokumentera redan existerande säkerhetsprocesser
3. Utforma och dokumentera nya säkerhetsprocesser

### Resultat

Resultatet är att tidigare existerande och nytillkomna säkerhetsprocesser är dokumenterade i form av en processbeskrivning. Beskrivningen visar i stort vad som skall göras, i vilken ordning, och av vem.

### Stöd

1. Beskrivning: Utforma säkerhetsprocesser – Metodstöd MSB, www.informationssäkerhet.se

## 5.3 Utforma policy och styrdokument

### Beskrivning

När alla nödvändiga säkerhetsåtgärder är fastställda och de säkerhetsprocesser som krävs är specificerade är det dags att ta fram verksamhetens styrande dokument. Policyn och de tillhörande styrande dokumenten är viktiga styrmedel i säkerhetsarbetet. De är grunden för att säkerhetsarbetet genomförs på ett strukturerat sätt och utgör en viktig utgångspunkt för granskning av informationssäkerhetsarbetet.

Det finns många gånger befintliga styrdokument inom kommunen och att identifiera dessa är viktigt för att veta vilket material man har att utgå ifrån. Här skapar man sig en bild av vilken arbetsinsats som krävs för att få den täckning man eftersträvar samt ordning och reda på styrdokumenten.

### Att göra

1. Utforma och fastställ informationssäkerhetspolicy
2. Identifiera befintliga dokument
3. Uppdatera dokument baserat på föregående aktivitet (Välj säkerhetsåtgärder)
4. Skriv nya dokument i de fall tidigare riktlinjer saknades

### Resultat

Resultatet är att verksamhetens policy och styrande dokument för informationssäkerhet är uppdaterade eller framtagna samt beslutade av ledningen. Dokumenten riktar sig till olika målgrupper och beskriver viljeinriktningen och förhållningsregler för informationssäkerheten.

### Stöd

1. Bilaga 1: Policy och Riktlinjer för Informationssäkerhet
2. Beskrivning: Utforma Policy och Styrande dokument – Metodstöd MSB, www.informationssäkerhet.se

# 6. Införa

## 6.1 Planera genomförande

### Beskrivning

Nu är det dags att ta fram en övergripande plan för införandet. Genom planen blir de olika aktiviteter som krävs för ett effektivt införande identifierade, genomtänkta och inplanerade i kalendern. Det blir också tydligt vilka resurser som krävs för de olika aktiviteterna. Om en projektplan för LIS-införandet togs fram inför genomförandet av de grundläggande analyserna är det nu dags att uppdatera och förtydliga den vad gäller införandet av de åtgärder som utformades under steget *Utforma LIS*.

I den första övergripande planeringen där helhet och därmed vissa strategiska vägval ska göras är det viktigt att ansvariga beslutsfattare inom informationssäkerhetsprojektet och linjeverksamheten är involverade. För att få en realistisk planering med hänsyn till helhetsperspektivet måste intressenter från verksamhetens olika delar delta. En ledare för införandet bör utses.

Det är viktigt att de som arbetar i verksamheten blir informerade om kommande förändringar, varför förändringar behövs och hur verksamheten kommer att tjäna på förändringarna. Därför är det bra att i planeringsskedet också utse en kommunikationsansvarig.

### Att göra

1. Planera med helhetsperspektiv
2. Konkretisera de fastställda säkerhetsåtgärderna och säkerhetsprocesserna till den grad att de kan planeras
3. Ta fram en tidsplan för införandet

### Resultat

Resultatet är en tidplan där införandet är inplanerat i tid, som även visar vad som skall göras, när och av vem.

### Stöd

1. Beskrivning: Planera Införande – Metodstöd MSB, www.informationssäkerhet.se

## 6.2 Konstruera och anskaffa

### Beskrivning

Flera av de säkerhetsåtgärder och säkerhetsprocesser som nu planerats behöver antingen konstrueras eller anskaffas. Med konstruktion avses det som utvecklas av organisationen själv, och med anskaffning menas sådant som köps in utifrån.

Vad som ska konstrueras och anskaffas framgår av den dokumenterade tidplanen. Där anges för varje säkerhetsåtgärd och säkerhetsprocess vilka aktiviteter som krävs för dess realisering. Det kan gälla ett beslutat intrångsdetekteringssystem som ska köpas in, installeras, konfigureras och införas. Det kan också vara en utbildning till medarbetarna som ska tas fram.

I konstruera och anskaffa ingår alla delaktiviteter som krävs för att realisera säkerhetsåtgärder och säkerhetsprocesser inför ett införande.

En viktig del är kravställning och brister i den är en vanlig orsak till att utvecklingsprojekt går fel. Om ett krav blir feltolkat, eller rentav helt glöms bort, är det väldigt kostsamt om det upptäcks först när det är färdigt. Eller ännu värre – då det är satt i drift. Utgå ifrån att kraven måste ses över under hela utvecklingsarbetet, även om förändringarna mot slutet bör vara små.

### Att göra

1. Specificera krav
2. Konstruera eller anskaffa säkerhetsåtgärden
3. Överlämna till införande

### Resultat

När alla komponenter är framtagna eller införskaffade ska de överlämnas till den som ansvarar för införandet. I den bästa av världar är alla komponenter testade och väldokumenterade och införandet av åtgärden i verksamheten kan genomföras enligt organisationen normala driftsättningsrutiner. I praktiken blir överlämnandet sällan helt smärtfritt och det kan vara bra om den utvecklingsansvarige (eller inköpsansvarige) har en viss beredskap att ge stöd även efter överlämnandet.

### Stöd

1. Beskrivning: Konstruera och Anskaffa – Metodstöd MSB, www.informationssäkerhet.se

## 6.3 Införa

### Beskrivning

Nu är alla säkerhetsåtgärder och säkerhetsprocesser framtagna eller införskaffade och det är dags att låta de göra nytta i verksamheten. En stor del av införandet handlar om teknik och administration. Men lika kritiskt för ett framgångsrikt införande är hur väl man får medarbetarna att ta till sig förändringarna. Det handlar mycket om pedagogik. För att åtgärder och processer ska få nytta i praktiken krävs att alla i verksamheten sluter upp bakom dem på bred front.

Vanliga reaktioner hos medarbetare när nya säkerhetsåtgärder och säkerhetsprocesser införs är:

- ”Inget vi har beställt” – en skepsis mot att införa något man själv inte har bett om eller tycker sig behöva.
- ”Vad ger det här mig?” – om förändringen innebär en (subtilt) krångligare vardag är det lätt att strunta i nya riktlinjer om man inte ser någon egen kortsiktig vinning.

Nyckeln till att komma förbi svårigheterna är att kommunicera vilka förändringarna blir och varför de införs. Det är viktigt att inte bli för teknisk i kommunikationen utan att hålla beskrivningarna på en användarnivå.

Med införande menas här de verksamhetsanpassningar som måste göras i organisationen. Exempel på sådana verksamhetsanpassningar är nya arbetssätt och rutiner, organisationsförändringar, nya roller och ansvar, utbildningar med mera. Den generella införandeprocessen ska vara ett stöd för hur de nödvändiga verksamhetsanpassningarna ska genomföras.

### Att göra

1. Förbereda införande
2. Anpassa organisation och arbetssätt
3. Kommunicera förändringar
4. Förbereda förvaltning, test och drift
5. Utbilda och träna
6. Driftsätta

### Resultat

Nu är verksamhetens sätt att styra och leda informationssäkerheten, inklusive beslutade säkerhetsåtgärder, införda. Olika grupper anställda har fått information och utbildning om policy och riktlinjer för informationssäkerhet. Arbetet med att etablera själva ledningssystemet är slutfört! Det som tar vid nu är övervakning och ständiga förbättringar.

### Stöd

1. Beskrivning: Införa – Metodstöd MSB, www.informationssäkerhet.se

# Bilagor

# Bilaga 1:
# Policy och Riktlinjer för Informationssäkerhet

### Framtagande av policy och riktlinjer

En övergripande policy är ledningens viljeyttring vad avser informationssäkerhetens inriktning. Riktlinjer för informationssäkerhet berättar för olika målgrupper i verksamheten vad som gäller. Dessa styrande dokument är grunden för att säkerhetsarbetet hanteras på ett strukturerat sätt. En viktig del i arbetet med att etablera en styrning över informationssäkerheten är att göra en översyn av befintliga policyer och riktlinjer för informationssäkerhet. I de fall sådana inte finns ska de tas fram, med utgångspunkt i verksamhetens behov. Dessa dokument är grunden för att säkerhetsarbetet hanteras på ett strukturerat sätt. De är också viktiga att ha för att kunna granska informationssäkerhetsarbetet.

### När ska policyn tas fram

En mer övergripande informationssäkerhetspolicy kan tas fram redan vid starten på projektet. Mer detaljerade styrdokument bör man vänta med tills åtminstone efter de grundläggande analyserna (under *verksamhetsanalys*, *riskanalys* och *gapanalys* i metodstödet) är genomförda. Styrande dokument som vilka beskriver olika säkerhetsåtgärder och säkerhetsprocesser tas lämpligen fram i samband med utformningen av dessa (under *utforma säkerhetsåtgärder* och *utforma säkerhetsprocesser* i metodstödet). Kommunikation och införande av dessa styrande dokument sker sedan vid implementeringen (under *införa* i metodstödet).

### Förankring i verksamheterna

En tjänsteman med kunskaper om kommunal verksamhet och informationssäkerhet leder normalt arbetet med att ta fram policy och riktlinjer för informationssäkerhet. De olika verksamheterna i kommunen konsulteras vid framtagandet, exempelvis enheterna för juridik, IT och personal samt andra verksamheter såsom utbildning, omsorg, stadsbyggnad. Detta för att se till att de principer och regler som tas fram är avpassade för de olika verksamheterna.

### Beslut om policy och riktlinjer

Kommunfullmäktige beslutar normalt om kommunövergripande policy för informationssäkerhet. Mer konkreta riktlinjer beslutas normalt inte av kommunfullmäktige utan kan beslutas av exempelvis kommunstyrelse, kommunledning eller kommundirektör.

### Rekommenderade områden i policyn

En policy visar högsta ledningens viljeinriktning gällande informationssäkerhet. Efter att ha läst hela policyn bör läsaren ha svar på följande frågor:

- Vad är informationssäkerhet, och varför ska vi ha det?
- Vilken är ledningens viljeinriktning och verksamhetens mål när det gäller informationssäkerhet?
- Vad är det jag förväntas göra, och var får jag mer information?

Dokumentet ska hållas kortfattat och helst under fem A4-sidor. Här följer rekommendationer på vilka områden som bör vara med i en informationssäkerhetspolicy.

### Allmänt

Detta område lägger grunden till policyn genom att förklara vad informationssäkerhet är, visar ledningens vilja, berättar om kraven och om hur policyn hänger ihop med andra styrande dokument. Följande frågor är aktuella:

- *Definition*: Vad informationssäkerhet är
- *Motiv*: Vikten av informationssäkerhet i verksamheten
- *Vilja*: Viljedeklaration från högsta ledningen avseende informationssäkerhet
- *Krav*: Listar viktiga krav, exempelvis lagkrav
- *Definitioner*: Definitioner av grundläggande begrepp som informationstillgångar, konfidentialitet, etc.

### Mål

Detta område ska ge grunden för att fastställa mål för informationssäkerhet.

– *Långsiktiga mål*: Det är vanligt att man direkt anger ett antal övergripande mål såsom målet att ”alla anställda har kunskap om gällande informationssäkerhetsregler”.
– *Kortsiktiga mål*: Eftersom policyn som dokument ska leva länge utan att behöva uppdateras, så är det ovanligt att direkt ange mer kortsiktiga (exempelvis årliga) mål direkt i dokumentet. Istället refererar man ofta till att sådana mål ska beslutas, exempelvis i samband med verksamhetsplaneringen i övrigt.

De kortsiktiga målen bör vara formulerade på ett sådant sätt att de är specifika, mätbara, motiverande för arbetet, realistiska och inplanerade i tid. Exempel på ett sådant mål kan vara ”Under 2015 ska minst 95 % av våra medarbetare och konsulter ha genomgått informationssäkerhetsutbildningen DISA”.

### Struktur

Detta område förklarar hur verksamheten och specifikt informationssäkerheten styrs. Informationen bör sätta in policyn i ett större sammanhang – verksamhetens ledning och styrning, samt förklara hur policyn tydliggörs med dokument på andra nivåer, exempelvis riktlinjer. Området kan även förklara hur olika delar av verksamheten, exempelvis olika bolag och förvaltningar, påverkas av policyn.

### Riktlinjer

Policyn är i sig ett övergripande dokument, vilket innebär att det måste tydliggöras i riktlinjer eller liknande dokument. Detta område i policyn listar riktlinjerna och anger på en mycket hög nivå säkerhetsmålet med respektive riktlinje. Vilka riktlinjer verksamheten väljer att ta fram beror på hur behovet ser ut. Följande riktlinjer är vanligen förekommande:

– *Riktlinjer för Användare/lathund*: De riktlinjer som riktar sig till användare, innefattandes medarbetare och uppdragstagare, sammanställs och presenteras i detta separata dokument. Exempel på sådana kan vara användning av e-post, surfning, virusskydd, rapportering av incidenter, påföljd vid ”brott” mot reglerna, etc.

- *Riktlinjer för förvaltningsledning.*
- *Riktlinjer för Skydd mot skadlig kod*: Upptäckande, förebyggande och återställande skydd mot skadlig kod ska finnas och lämpliga rutiner ska införas för att uppmärksamma användarna.
- *Riktlinjer för Incidenthantering*: Informationssäkerhetsincidenter ska inrapporteras via fastställda rapporteringsvägar. Alla anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster ska notera och rapportera alla observerade eller misstänkta säkerhetsbrister i system eller tjänster.
- *Riktlinjer för Ändringshantering*: Införandet av mer genomgripande förändringar i IT-systemen ska styras genom användning av den fastställda rutinen för ändringshantering.
- *Riktlinjer för Loggning*: Loggar ska produceras i den utsträckning som krävs för att verksamheten ska kunna förebygga, upptäcka och rätta till relevanta fel och felaktigheter, oönskade händelser och förändringar i nätverk, IT- system, programvara och information.
- *Riktlinjer för Säkerhetskopiering*: Säkerhetskopior av information och programvara ska tas och testas regelbundet i enlighet med fastställda riktlinjer.
- *Riktlinjer för Åtkomst*: Åtkomst till informationstillgångar ska beredas i den utsträckning som krävs för att anställda och uppdragstagare ska kunna ändamålsenligt genomföra sina arbetsuppgifter samt leva upp till krav som ställs i avtal och författningar.
- *Riktlinjer för Behörighetsadministration*: Formella rutiner för registrering av användare och tilldelning av lösenord för att medge och återkalla åtkomst till alla informationssystem och tjänster ska användas.
- *Riktlinjer för Mobilt arbete*: Vid arbete med mobila enheter, som t.ex. bärbar dator, mobiltelefon och USB-minnen, på annat ställe än i de egna lokalerna finns särskilda riktlinjer för informationssäkerhet. Uppgifter av känslig natur får endast hanteras på mobil enhet försedd med fil- eller diskkryptering.
- *Riktlinjer för Inventarier och licenser*: Aktuella förteckningar ska föras över IT-tillgångar samt användning av programvarulicenser. Detta innefattar lista på servrar, klientdatorer, nätverksenheter och programvaror.

– *Riktlinjer för Fysisk säkerhet*: Den fysiska säkerheten skall organiseras så att verksamhetens personal och uppdragstagare, lokaler, utrustning och informationsresurser skyddas mot hot som inbrott, stöld, brand, översvämning, olyckor och katastrofer som orsakas av fel i tekniska system, misstag, sabotage eller andra externa händelser.
– *Riktlinjer för Kontinuitetsplanering*: Kontinuitetsplaner för kritiska verksamhetsprocesser ska upprättas, testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla. Syftet är att motverka avbrott i organisationens verksamhet och för att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer.
– *Riktlinjer för Utbildning*: Alla anställda och uppdragstagare ska årligen ges en kort utbildning i informationssäkerhet med särskild inriktning på denna policy och riktlinjer samt vikten av att följa reglerna. Information ges även i samband med att nya personer engageras i verksamheten.

### Organisation

Detta område i policyn utvisar vem som ansvarar för vad när det gäller informationssäkerhet, det vill säga verksamhetens säkerhetsorganisation. Det är viktigt att det personliga ansvaret beskrivs tydligt, så att läsaren vet vad som förväntas. Därefter är det viktigt att organisationen beskrivs med tillräcklig tydlighet så att läsaren kan förstå vem som ansvarar för vad.

Ofta beskriver man ett antal roller kopplat till informationssäkerheten, exempelvis informationssäkerhetsansvarig, informationsägare, medarbetare, för att därefter ange vilket ansvar de har i informationssäkerhetsarbetet. Ett sätt att presentera organisationen på är genom en tabell med kolumner för ”roll”, ”ansvar” och ”uppgifter”.

Vilka roller som definieras och hur de olika ansvaren och uppgifterna beskrivs beror på behovet i verksamheten.

### Uppföljning och rapportering

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att beslutade åtgärder är genomförda, att årliga mål är uppfylls, att regler följs, att policy, säkerhetsinstruktioner och analyser vid behov görs om eller ses över. Området om uppföljning och rapportering bör ange vem som ska följa upp vad och hur det ska rapporteras.

# Bilaga 2: Informationstillgångar

**Informationstillgångar i kommuner**

En undersökning hos flera kommuner genomförd av MSB visade att dessa informationstillgångar ofta förekommer.

| | | | | | |
|---|---|---|---|---|---|
| Diariet | Patient journal | Bokningssystem | Föreningsregister | Låntagarregister | Personakter |
| Utbetalningar | Extern webbplats | Dokumenattion inom social omsorg | Kartdatabas | Ritningsarkiv | Bygglov |
| Tomt- och huskö | Styrsystem för vatten och avlopp | Schemaläggning | Skolhälsovård | Elevregister | Betyg |
| Personaldossier | Personalregister | Lönesystem | Tidrapportering | Redovisning | Verksamhetsplan |
| Avtal | Anläggningsregister | Fakturering | Reskontra | Telefonväxeln | Active Directory |
| Befolkningsregister | Klientdatorer | Servrar | Nätverk | E-postsystem | Webbservrar |

# Bilaga 3: Säkerhetsåtgärder

De här säkerhetsåtgärderna kommer från den internationella standarden ISO/IEC 27001 och följer dess numrering. Mer information om varje säkerhetsåtgärd i listan kan erhållas i standarden ISO/IEC 27002. Kommunen bör överväga ifall dessa säkerhetsåtgärder behövs samt om skyddet blir komplett eller om andra åtgärder utöver dessa krävs. För flertalet organisationer passar alla eller nästan alla åtgärder. Denna bilaga används vid olika steg i metodstödet, exempelvis vid GAP-analys samt val och utformning av säkerhetsåtgärder och säkerhetsprocesser.

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **5** | **1** | **1** | Policydokument för informationssäkerhet | Ett policydokument för informationssäkerhet skall godkännas av ledningen samt publiceras och kommuniceras till alla anställda och till relevanta externa parter. |
| **5** | **1** | **2** | Granskning av informations-säkerhetspolicyn | Informationssäkerhetspolicyn skall granskas vid planerade intervall, eller om betydande ändringar inträffar, för att säkerställa dess fortsatta lämplighet, tillräcklighet och verkan. |
| **6** | **1** | **1** | Ledningens engagemang för informationssäkerhet | Ledningen skall aktivt stödja säkerheten inom organisationen genom tydlig inriktning, påvisat engagemang, tydlig fördelning och bekräftelse av ansvar för informationssäkerhet. |
| **6** | **1** | **2** | Samordning av informations-säkerhetsarbetet | Aktiviteter som rör informationssäkerhet skall samordnas av representanter från olika delar av organisationen med relevanta roller och arbetsuppgifter. |
| **6** | **1** | **3** | Tilldelning av ansvar för informationssäkerhet | Allt informationssäkerhetsansvar skall vara klart definierat. |
| **6** | **1** | **4** | Godkännandeprocess för informations-behandlingsresurser | En driftsgodkännandeprocess för nya informations-behandlingsresurser skall definieras och införas. |
| **6** | **1** | **5** | Konfidentialitetsavtal | Krav på konfidentialitetsavtal eller NDA som lever upp till verksamhetens krav ska finnas. |
| **6** | **1** | **6** | Myndighetskontakt | Lämpliga kontakter skall upprätthållas med relevanta myndigheter. |
| **6** | **1** | **7** | Kontakt med särskilda intressegrupper | Lämpliga kontakter skall upprätthållas med särskilda intressegrupper eller andra forum och yrkesorganisationer för säkerhetsspecialister. |
| **6** | **1** | **8** | Oberoende granskning av informationssäkerhet | Organisationens metod för att hantera informations-säkerhet och dess tillämpning (t.ex. åtgärdsmål, säkerhetsåtgärder, policyer, processer och rutiner för informationssäkerhet) skall granskas oberoende med planerade mellanrum eller när det inträffar väsentliga förändringar som berör tillämpningen av säkerheten. |
| **6** | **2** | **1** | Identifiering av risker med utomstående parter | Riskerna för organisationens information och informationsbehandlingsresurser i verksamhetsprocesser där utomstående parter är involverade skall identifieras och lämpliga säkerhetsåtgärder införas innan åtkomst beviljas. |
| **6** | **2** | **2** | Hantering av säkerhet vid kundkontakter | Alla identifierade säkerhetskrav skall behandlas innan kunder ges åtkomst till organisationens information eller andra tillgångar. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **6** | **2** | **3** | Hantering av säkerhet i tredjepartsavtal | Avtal med en tredje part omfattande åtkomst, bearbetning, kommunikation och hantering av organisationens information eller informationsbehandlingsresurser, alternativt tillägg av produkter eller tjänster till informationsbehandlingsresurserna skall omfatta alla relevanta säkerhetskrav. |
| **7** | **1** | **1** | Förteckning över tillgångar | Alla tillgångar skall tydligt märkas och en förteckning omfattande alla viktiga tillgångar skall upprättas och underhållas. |
| **7** | **1** | **2** | Ägarskap för tillgångar | All information och tillgångar som hör till informationsbehandlingsresurserna skall ”ägas” 1) av en utsedd organisationsenhet. |
| **7** | **1** | **3** | Godtagbar användning av tillgångar | Regler för hur information och tillgångar tillhörandes informationsbehandlingsresurser får användas skall utformas, dokumenteras och införas. |
| **7** | **2** | **1** | Riktlinjer för klassificering | Information skall klassificeras i termer av dess värde, legala krav, känslighet och betydelse för organisationen. |
| **7** | **2** | **2** | Märkning och hantering av information | En lämplig uppsättning rutiner för märkning och hantering av information skall utvecklas och införas i enlighet med det klassificeringssystem som antagits av organisationen. |
| **8** | **1** | **1** | Roller och ansvar | Anställdas, uppdragstagares och utomstående användares roller och ansvar skall definieras och dokumenteras i enlighet med organisationens informationssäkerhetspolicy. |
| **8** | **1** | **2** | Kontroll av personal | Verifiering av personens bakgrund skall göras för alla rekryteringskandidater, uppdragstagare och tredjepartsanvändare i enlighet med relevanta författningar och etiska regler. Kontrollerna skall stå i proportion till organisationens krav, klassificeringen av den information för vilken åtkomst behövs och de uppfattade riskerna. |
| **8** | **1** | **3** | Anställningsvillkor | Som en del av sina avtalsskyldigheter skall anställda, uppdragstagare och utomstående användare godta och underteckna de villkor och förhållanden i anställningsavtalet som skall ange det egna och organisationens ansvar för informationssäkerhet. |
| **8** | **2** | **1** | Ledningens ansvar | Ledningen skall kräva att anställda, uppdragstagare och tredjepartsanvändare tillämpar säkerhet i enlighet med organisationens beslutade policyer och rutiner. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **8** | **2** | **2** | Informationssäkerhets-medvetande, utbildning och övning | Alla organisationens anställda och, där det är relevant, uppdragstagare och tredjepartsanvändare skall få erforderlig utbildning och regelbunden uppdatering om organisationens policyer och rutiner som är relevanta för deras arbetsuppgifter. |
| **8** | **2** | **3** | Disciplinär process | Det skall finnas en formell disciplinär process för anställda som har åsidosatt säkerheten. |
| **8** | **3** | **1** | Ansvar vid upphörande av anställning | Ansvaret för att avsluta eller förändra anställning skall vara klart definierat och tilldelat. |
| **8** | **3** | **2** | Återlämnande av tillgångar | Alla anställda, uppdragstagare och tredjepartsanvändare skall återlämna alla organisationens tillgångar som de innehar när anställningen, avtalet eller överenskommelsen upphör. |
| **8** | **3** | **3** | Indragning av åtkomst-rättigheter | Alla anställdas, uppdragstagares och tredjeparts-användares åtkomsträtt till information och informations-behandlingsresurser skall dras in när anställningen, avtalet eller överenskommelsen upphör, eller justeras vid förändringar. |
| **9** | **1** | **1** | Skalskydd | Skalskydd (avspärrningar som väggar, kortstyrda entréer eller bemannade receptioner) skall användas för att skydda utrymmen där information och informations-behandlingsresurser finns. |
| **9** | **1** | **2** | Tillträdeskontroll | Säkra utrymmen skall skyddas genom lämpliga tillträdes-kontroller för att säkerställa att endast behörig personal får tillträde. |
| **9** | **1** | **3** | Skydd för kontor, rum och faciliteter | Kontor, rum och faciliteter bör utformas med tanke på fysisk säkerhet. |
| **9** | **1** | **4** | Skydd mot externa hot och miljöhot | Fysiska skydd mot skada orsakad av brand, översvämning, jordbävning, explosion, upplopp och andra former av naturliga eller av människor orsakade katastrofer skall utformas och användas. |
| **9** | **1** | **5** | Arbete i säkra utrymmen | Fysiskt skydd och riktlinjer för arbete i säkra utrymmen skall utformas och tillämpas. |
| **9** | **1** | **6** | Allmänhetens till-träde, leverans- och lastutrymmen | Platser för tillträde som, t.ex. leverans- och lastutrymmen och andra platser där obehöriga personer kan komma in i lokalerna skall övervakas och, om möjligt, avskärmas från informationsbehandlingsresurser för att undvika obehörigt tillträde. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **9** | **2** | **1** | Placering och skydd av utrustning | Utrustning skall placeras eller skyddas för att minska risken för miljömässiga hot och faror och för möjligheten till obehörig åtkomst. |
| **9** | **2** | **2** | Tekniska försörjnings-system | Utrustning skall skyddas mot elavbrott och andra störningar orsakade av avbrott i tekniska försörjningssystem. |
| **9** | **2** | **3** | Kablageskydd | Både starkströms- och telekommunikationskablar som används för datatrafik eller stödjer informationstjänster skall skyddas mot avlyssning och åverkan. |
| **9** | **2** | **4** | Underhåll av utrustning | Utrustning skall underhållas på korrekt sätt för att säkerställa dess fortsatta tillgänglighet och systemintegritet. |
| **9** | **2** | **5** | Säkerhet för utrustning utanför egna lokaler | Säkerhet beträffande utrustning utanför egna lokaler skall utformas med de olika risker som är förknippade med arbeta utanför organisationens lokaler i åtanke. |
| **9** | **2** | **6** | Säker avveckling eller återanvändning av utrustning | Alla utrustningsenheter som är försedda med lagringsmedia skall kontrolleras för att säkerställa att alla känsliga data och licensierade program har tagits bort eller överskrivits på ett säkert sätt innan utrustningen avvecklas. |
| **9** | **2** | **7** | Avlägsnande av egendom | Utrustning, information eller program skall inte avlägsnas från organisationens lokaler utan föregående tillstånd. |
| **10** | **1** | **1** | Dokumenterade driftrutiner | Driftrutiner skall dokumenteras, underhållas och göras tillgängliga för alla användare som behöver dem. |
| **10** | **1** | **2** | Ändringshantering | Förändringar av informationsbehandlingsresurser och system skall styras. |
| **10** | **1** | **3** | Uppdelning av arbetsuppgifter | Arbetsuppgifter och ansvar skall åtskiljas för att minska tillfällen till obehörig eller oavsiktlig förändring eller missbruk av organisationens tillgångar. |
| **10** | **1** | **4** | Uppdelning av utvecklings- test- och driftresurser | Utvecklings- , test- och driftresurser skall åtskiljas för att minska risken för obehörig åtkomst till eller ändringar i driftsystem. |
| **10** | **2** | **1** | Tjänsteleverans | Det skall säkerställas att säkerhetsåtgärder, definitioner av tjänsten och leveransnivån enligt avtalet med den tredje parten införs, drivs och upprätthålls av parten ifråga. |
| **10** | **2** | **2** | Övervakning och granskning av tjänster från tredje part | De tjänster, rapporter och redovisningar som presteras av tredje part skall regelbundet övervakas och granskas och revisioner skall göras regelbundet. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **10** | **2** | **3** | Ändringshantering av tjänster från tredje part | Ändring av utförande av tjänster, inklusive att upprätthålla och förbättra befintliga policyer, rutiner och säkerhetsåtgärder för informationssäkerhet, skall hanteras med hänsyn till hur kritiska verksamhetssystem och processer är och till förnyad bedömning av risker. |
| **10** | **3** | **1** | Kapacitetsplanering | Resursanvändningen skall övervakas, justeras, och prognoser bör göras av framtida kapacitetskrav för att säkerställa den erforderliga prestandan i systemen. |
| **10** | **3** | **2** | Systemgodkännande | Kriterier för godkännande av nya och uppgraderade informationssystem liksom för nya versioner skall fastställas och lämpliga tester av system(en) utföras under utvecklingen och före godkännande. |
| **10** | **4** | **1** | Säkerhetsåtgärder mot skadlig kod | Upptäckande, förebyggande och återställande säkerhetsåtgärder skall införas för att skydda mot skadlig kod och lämpliga rutiner skall införas för att uppmärksamma användarna. |
| **10** | **4** | **2** | Säkerhetsåtgärd mot mobil kod | Där användning av mobil kod är tillåten skall konfigurationen säkerställa att godkänd mobil kod fungerar enligt en tydligt definierad säkerhetspolicy och att exekvering av icke godkänd mobil kod förhindras. |
| **10** | **5** | **1** | Säkerhetskopiering av information | Säkerhetskopior av Information och programvara skall tas och testas regelbundet i enlighet med den beslutade policyn för säkerhetskopiering. |
| **10** | **6** | **1** | Säkerhetsåtgärder för nätverk | Nätverk skall vara adekvat administrerade och övervakade, för att vara skyddade från hot, och för att upprätthålla säkerhet för system och tillämpningar som nyttjar nätverket, innefattandes även information under överföring. |
| **10** | **6** | **2** | Säkerhet i nätverkstjänster | Säkerhetsegenskaper, tjänstenivåer och förvaltningskrav för alla nätverkstjänster skall klarläggas och ingå i varje överenskommelse om nätverkstjänster, oavsett om dessa tjänster utförs inom organisationen eller är utlagda. |
| **10** | **7** | **1** | Hantering av flyttbara datamedia | Det skall finnas rutiner för hantering av flyttbara datamedia. |
| **10** | **7** | **2** | Avveckling av media | Media skall avvecklas på ett säkert och ofarligt sätt enligt en formell rutin när de inte längre behövs. |
| **10** | **7** | **3** | Rutiner för informationshantering | Rutiner skall upprättas för hantering och förvaring av information i syfte att skydda sådan information mot obehörigt avslöjande eller användning. |
| **10** | **7** | **4** | Säkerhet för systemdokumentation | Systemdokumentation skall skyddas mot obehörig åtkomst. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **10** | **8** | **1** | Policyer och rutiner för informationsutbyte | Formella policyer, rutiner och säkerhetsåtgärder för informationsutbyte skall finnas för att skydda utbyte av information via alla typer av kommunikationsvägar. |
| **10** | **8** | **2** | Överenskommelser om utbyte | Överenskommelser om utbyte av information och programvara mellan organisationen och externa parter skall upprättas. |
| **10** | **8** | **3** | Fysiska media under transport | Media som innehåller information skall skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport utanför en organisations fysiska gränser. |
| **10** | **8** | **4** | Elektroniska meddelanden | Information som hanteras i elektroniskt meddelande skall skyddas på lämpligt sätt. |
| **10** | **8** | **5** | Verksamhetsrelaterade informationssystem | Policyer och rutiner skall utvecklas och införas för att skydda information i samband med sammankoppling av verksamhetsrelaterade informationssystem. |
| **10** | **9** | **1** | Elektronisk handel | Information inbegripen i elektronisk handel som skickas över allmänt tillgängliga nätverk skall skyddas mot bedrägliga förfaranden, avtalstvister, samt obehörigt avslöjande, och modifiering. |
| **10** | **9** | **2** | Direktanslutna transaktioner | Information i direktanslutna (on-line) transaktioner skall skyddas för att förhindra ofullständig överföring, fel-adressering, obehörig ändring av meddelande, obehörigt avslöjande, obehörig duplicering eller repetition av meddelande. |
| **10** | **9** | **3** | Offentligt tillgänglig information | Riktigheten hos information som görs tillgänglig i ett för allmänheten tillgängligt system bör skyddas för att förhindra obehörig modifiering. |
| **10** | **10** | **1** | Revisionsloggning | Revisionsloggar som registrerar användaraktiviteter, undantag, och informationssäkerhetshändelser skall föras och bevaras under en bestämd tidsperiod för att vara till hjälp vid framtida undersökningar och övervakning av åtkomstkontroll. |
| **10** | **10** | **2** | Övervakning av systemanvändning | Rutiner för övervakning av informationsbehandlingsresursernas användning skall upprättas och övervakningsresultaten granskas regelbundet. |
| **10** | **10** | **3** | Skydd av logg-information | Loggningsresurser och logginformation skall skyddas mot manipulering och obehörig åtkomst. |
| **10** | **10** | **4** | Administratörs- och operatörsloggar | Systemadministratörers och systemoperatörers aktiviteter skall loggas. |
| **10** | **10** | **5** | Loggning av fel | Fel skall loggas, analyseras och lämpliga åtgärder vidtas. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **10** | **10** | **6** | Klocksynkronisering | Klockor i alla relevanta informationsbehandlingssystem inom en organisation eller en säkerhetsdomän skall synkroniseras med en överenskommen korrekt tidsangivelse. |
| **11** | **1** | **1** | Åtkomstpolicy | En åtkomstpolicy skall fastställas, dokumenteras och granskas baserat på verksamhets- och säkerhetskrav gällande åtkomst. |
| **11** | **2** | **1** | Användarregistrering | Det skall finnas en formell rutin för registrering och avregistrering för att medge och återkalla åtkomst till alla informationssystem och tjänster. |
| **11** | **2** | **2** | Hantering av särskilda rättigheter | Tilldelning och användning av privilegierad åtkomsträtt skall begränsas och styras. |
| **11** | **2** | **3** | Lösenordshantering | Tilldelning av lösenord skall styras genom en formell administrativ process. |
| **11** | **2** | **4** | Granskning av användares åtkomsträttigheter | Ansvariga chefer skall granska användares åtkomsträttigheter med jämna mellanrum genom en formell process. |
| **11** | **3** | **1** | Användning av lösenord | Användare skall följa god säkerhetssed vid val och användning av lösenord. |
| **11** | **3** | **2** | Obevakad användarutrustning | Användare skall säkerställa att obevakad utrustning har tillräckligt skydd. |
| **11** | **3** | **3** | Policy för renstädat skrivbord och tom bildskärm | En policy för renstädat skrivbord utan pappersdokument och flyttbara datamedia liksom en policy för tom bildskärm för informationsbehandlingsresurser, skall antas. |
| **11** | **4** | **1** | Policy för användning av nätverkstjänster | Användare skall förses med åtkomst endast till de tjänster som de särskilt fått behörighet att använda. |
| **11** | **4** | **2** | Autentisering av användare vid extern anslutning | Lämpliga autentiseringsmetoder skall användas för att styra fjärranvändares åtkomst. |
| **11** | **4** | **3** | Identifiering av utrustning i nätverk | Automatisk identifiering av utrustning skall övervägas som en metod att autentisera anslutningar från olika platser och utrustningar. |
| **11** | **4** | **4** | Skydd av extern diagnos- och konfigurationsport | Fysisk och logisk åtkomst till diagnos- och konfigurationsportar skall styras. |
| **11** | **4** | **5** | Nätverkssegmentering | Grupper av informationstjänster, användare och informationssystem skall åtskiljas i nätverk. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **11** | **4** | **6** | Styrning av nätverks-anslutning | När det gäller delade nätverk, särskilt sådana som sträcker sig över organisationsgränser, skall användares möjligheter att ansluta sig till nätverket begränsas i enlighet med åtkomstpolicyn och verksamhetstillämpningarnas krav (se 11.1.1). |
| **11** | **4** | **7** | Styrning av routning | Säkerhetsåtgärder för routning skall införas för nätverk för att säkerställa att datoruppkopplingar och informationsflöden inte bryter mot åtkomstpolicyn till verksamhetstillämpningarna. |
| **11** | **5** | **1** | Säker påloggningsrutin | Åtkomst till operativsystem skall styras genom en säker påloggningsrutin. |
| **11** | **5** | **2** | Identifiering och autentisering av användare | Varje användare skall ha en unik identifikation (användar-ID) enbart för sin personliga användning och en lämplig autentiseringsteknik skall väljas för att styrka användarens uppgivna identitet. |
| **11** | **5** | **3** | Lösenordsrutin | System för att hantera lösenord skall vara interaktiva och skall säkerställa lösenord av god kvalitet. |
| **11** | **5** | **4** | Användning av systemverktyg | Användning av systemverktyg som kan förbigå system- och tillämpningsspärrar skall användas restriktivt och styras noga. |
| **11** | **5** | **5** | Tidsfördröjd nedkoppling | Inaktiva sessioner skall kopplas ned efter en fastställd period av inaktivitet. |
| **11** | **5** | **6** | Begränsning av uppkopplingstid | Begränsning av uppkopplingstid skall användas för att ge ytterligare säkerhet vid högrisktillämpningar. |
| **11** | **6** | **1** | Begränsning av åtkomst till information | Användares och underhållspersonals åtkomst till information och tillämpningssystemets funktioner skall begränsas i enlighet med den definierade åtkomstpolicyn. |
| **11** | **6** | **2** | Isolering av känsliga system | Känsliga system skall ha en dedikerad (isolerad) IT-miljö. |
| **11** | **7** | **1** | Mobil datoranvändning och kommunikation | En formell policy skall finnas och lämpliga säkerhetsåtgärder tillämpas för att skydda mot riskerna med att använda mobil bearbetnings- och kommunikationsutrustning. |
| **11** | **7** | **2** | Distansarbete | Policy, driftsplan och rutiner skall utformas och införas för distansarbetsaktiviteter. |
| **12** | **1** | **1** | Analys och specifikation av säkerhetskrav | Uttalanden om verksamhetens krav på nya informationssystem eller förbättring av befintliga informationssystem skall specificera kraven gällande säkerhetsåtgärder. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **12** | **2** | **1** | Validering av indata | Indata till tillämpningssystem skall valideras för att säkerställa att de är riktiga och relevanta. |
| **12** | **2** | **2** | Styrning av intern bearbetning | Valideringskontroller skall läggas in i systemen för att upptäcka eventuella förvanskningar av informationen genom bearbetningsfel eller med avsikt. |
| **12** | **2** | **3** | Meddelandeintegritet | Krav på att säkerställa autenticitet och skydda meddelandens riktighet i tillämpningar skall fastställas och lämpliga säkerhetsåtgärder fastställas och införas. |
| **12** | **2** | **4** | Validering av utdata | Utdata från ett tillämpningssystem skall valideras för att säkerställa att bearbetning av lagrad information är korrekt och lämplig med hänsyn till omständigheterna. |
| **12** | **3** | **1** | Krypteringspolicy | En policy för användning av kryptografiska säkerhetsåtgärder för informationsskydd skall utvecklas och införas. |
| **12** | **3** | **2** | Nyckelhantering | Ett nyckelhanteringssystem skall finnas för att stödja organisationens användning av krypteringsteknik. |
| **12** | **4** | **1** | Styrning av program i drift | Det skall finnas rutiner för att styra installation av program i driftsystem. |
| **12** | **4** | **2** | Skydd av testdata | Testdata skall väljas med noggrannhet, skyddas och styras. |
| **12** | **4** | **3** | Styrning av åtkomst till källprogramkod | Åtkomst till källprogramkod skall begränsas. |
| **12** | **5** | **1** | Rutiner för ändringshantering | Införandet av förändringar skall styras genom användning av en formell rutin för ändringshantering. |
| **12** | **5** | **2** | Teknisk granskning av tillämpningar efter ändringar i operativsystem | När operativsystem ändras skall verksamhetskritiska tillämpningar granskas och testas för att säkerställa att ändringen inte har negativ påverkan på organisationens drift eller säkerhet. |
| **12** | **5** | **3** | Restriktioner mot ändringar i programpaket | Modifieringar av programpaket skall minimeras, begränsas till nödvändiga ändringar, och alla ändringar skall strikt styras. |
| **12** | **5** | **4** | Informationsläckor | Möjlighet till informationsläckor skall förhindras. |
| **12** | **5** | **5** | Utlagd programvaruutveckling | Utlagd programvaruutveckling skall kontrolleras och övervakas av organisationen. |
| **12** | **6** | **1** | Skydd för tekniska sårbarheter | Information vid rätt tidpunkt om den tekniska sårbarheten hos informationssystem i drift skall inhämtas, organisationens utsatthet för sådan sårbarhet bedömas, och lämpliga åtgärder vidtas för att hantera den tillhörande risken. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **13** | **1** | **1** | Rapportering av informations-säkerhetshändelser | Informationssäkerhetshändelser skall inrapporteras via lämpliga rapporteringsvägar så snart som möjligt. |
| **13** | **1** | **2** | Rapportering av säkerhetsbrister | Det skall krävas av alla anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster att de noterar och rapporterar alla observerade eller misstänkta säkerhetsbrister i system eller tjänster. |
| **13** | **2** | **1** | Ansvar och rutiner | Ledningsansvar och rutiner skall fastställas för att säkerställa en snabb, verkningsfull och ordnad respons vid informations-säkerhetsincidenter. |
| **13** | **2** | **2** | Att lära av informations-säkerhetsincidenter | Det skall finnas metoder för att möjliggöra kvantifiering och övervakning av typer,volymer och kostnader för informationssäkerhetsincidenter. |
| **13** | **2** | **3** | Insamling av bevis | Då en uppföljande åtgärd mot en person eller organisation efter en informationssäkerhetsincident innefattar en juridisk åtgärd (civil- eller brottmål) skall bevis insamlas, bevaras och presenteras i överensstämmelse med bevis-regler i den eller de relevanta jurisdiktionerna. |
| **14** | **1** | **1** | Att inkludera informations-säkerhet i verksamhetens kontinuitetsplanerings-process | En ledningsprocess för kontinuitetsplanering i hela verksamheten skall utvecklas och underhållas. Denna process skall behandla de informationssäkerhetskrav som behövs för att hålla organisationens verksamhet i kontinuitet. |
| **14** | **1** | **2** | Kontinuerlig verksamhet och riskbedömning | Händelser som kan orsaka avbrott i verksamhetsprocesser skall identifieras tillsammans med sannolikheten och effekten av sådana avbrott och deras konsekvenser för informationssäkerheten |
| **14** | **1** | **3** | Utveckling och införande av kontinuitetsplaner innefattandeinformations-säkerhet | Planer skall utarbetas och införas för att upprätthålla eller återställa drift och säkerställa tillgänglighet till information på den nivå som krävs och inom erforderlig tid efter avbrott eller fel i kritiska verksamhetsprocesser. |
| **14** | **1** | **4** | Metodstöd för kontinuitetsplanering i verksamheten | Ett samlat ramverk för kontinuitetsplanering skall finnas för att säkerställa att alla planer är konsekventa, att informationssäkerhetskraven behandlas konsekvent och för att fastställa prioriteringar gällande test och underhåll. |
| **14** | **1** | **5** | Test, underhåll och omprövning av kontinuitetsplaner | Kontinuitetsplaner för verksamheten skall testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla. |
| **15** | **1** | **1** | Identifiering av tillämplig lagstiftning | Tillämpliga krav i författningar och i avtal liksom organisationens sätt att uppfylla dessa krav skall explicit definieras, dokumenteras och hållas uppdaterade för varje informationssystem och för organisationen som helhet. |

| AVSNITT | | | SÄKERHETSÅTGÄRD | BESKRIVNING |
|---|---|---|---|---|
| **15** | **1** | **2** | Immaterialrätt | Lämpliga åtgärder skall vidtas för att säkerställa efterlevnad av krav i författningar och avtal när det gäller användning av material för vilka immaterialrätt kan gälla och även ifråga om användning av upphovsrättsskyddade programvaror. |
| **15** | **1** | **3** | Skydd av organisationens register och andra redovisande dokument | Organisationens viktiga register och andra redovisande dokument skall skyddas mot förlust, förstörelse och förfalskning i enlighet med författnings-, avtals- och verksamhetskrav. |
| **15** | **1** | **4** | Skydd av personuppgifter | Data- och integritetsskydd skall säkerställas i enlighet med relevant lagstiftning och, där det är tillämpligt, avtalsklausuler. |
| **15** | **1** | **5** | Förhindrande av missbruk av informationsbehandlingsresurser | Användare skall avrådas från att använda informationsbehandlingsresurser för obehöriga ändamål. |
| **15** | **1** | **6** | Reglering av kryptering | Kryptering skall användas i enlighet med alla relevanta avtal och författningar. |
| **15** | **2** | **1** | Efterlevnad av säkerhetspolicyer och -standarder | Chefer skall säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområden utförs korrekt för att uppnå efterlevnad av säkerhetspolicyer och -standarder. |
| **15** | **2** | **2** | Kontroll av teknisk efterlevnad | Informationssystem skall regelbundet kontrolleras vad avser efterlevnad av standarder för införande av säkerhet. |
| **15** | **3** | **1** | Styrning av revision av informationssystem | Revisionens krav och åtgärder som innefattar kontroller av system i drift skall planeras noggrant och godkännas för att minimera risken för störningar i verksamhetsprocesser. |
| **15** | **3** | **2** | Skydd av verktyg för granskning av informationssystem | Åtkomst till granskningsverktyg för informationssystem skall begränsas för att hindra eventuellt missbruk och otillåten påverkan. |

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad  Tel 0771-240 240  www.msb.se
Publ.nr MSB508 - december 2012  ISBN 978-91-7383-304-2