Vårgårda kommun


# Riktlinjer för informationssäkerhet

**Beslutat av:** Kommunstyrelsen
**Datum för beslut: 2018-10-24**
**För revidering ansvarar:** Kommunstyrelsen
**Ansvarig verksamhet:** Strategisk planering och utveckling
**Ansvarig tjänsteman:** Chef strategisk planering och utveckling
**Dokumentet gäller för:** Anställda och förtroendevalda i Vårgårda kommun
**Dokumentet gäller till och med:** 2022-10-24, revidering vid behov

# Innehållsförteckning

# Riktlinjer för informationssäkerhet

Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

Riktlinjerna är en konkretisering av informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen.

## Riktlinjernas omfattning

Information och bestämmelser gällande säkerhet vid all hantering av information inom Vårgårda kommun. Riktlinjerna gäller för alla verksamheter vilket innebär att det inte finns utrymme att besluta om lokala regler som avviker från dessa.

Riktlinjerna gäller inte för kommunens bolag. Dessa beslutar om detta inom egen verksamhet. I vissa fall kan dessa riktlinjer gälla för kommunala bolag om, när de använder sig av kommunens informationsobjekt, eller då det finns behov av samordning.

## Struktur och läsanvisningar

För att ge god läsbarhet är dokumentet uppdelat i fyra kapitel som riktar sig till olika målgrupper.

| Kapitel | | Innehåll | Primär målgrupp | Sidor |
|---|---|---|---|---|
| A | Styrning av informationssäkerhet | Ansvarsfördelning för informationssäkerhet. Information och riktlinjer för hur arbetet med informationssäkerhet ska bedrivas | Alla som arbetar med IT- och informationssäkerhet | 12-24 |
| B | Informationssäkerhet för medarbetare | Information och riktlinjer för hur information och IT ska hanteras i olika situationer | Alla medarbetare | 25-34 |
| C | Informationssäkerhet i verksamhet och förvaltning | Information och riktlinjer för informationssäkerhet i som system och grupper av system | Informationsägare, objektsägare och systemägare | 39-45 |
| D | Informationssäkerhet i IT-miljön | Information och riktlinjer för hur information och IT ska hanteras inom IT-miljön, dvs. IT-säkerhet | Chefer och medarbetare på IT-avdelningen | 46-76 |

Varje kapitel består av information och riktlinjer som är obligatoriska. Samtliga riktlinjer är numrerade och i tabellform med ljusblått huvud. Rader i tabeller som innehåller riktlinjer för konfidentiell information och höga

skyddskrav har dubbla linjer. Exempel från kapitel A om Riktlinjer för personalsäkerhet före och i samband med anställning:

| Riktlinjer för personalsäkerhet före och i samband med anställning | |
|---|---|
| A.5.1 | Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras. |
| A.5.5 | Anställda som får tillgång till **konfidentiell** information ska underteckna ett sekretessavtal. |

Kapitel B – Informationssäkerhet för medarbetare – har strukturerats för att stämma överens med avsnitten i utbildningen DISA (Datorstödd informationssäkerhetsutbildning för användare). DISA-utbildningen kan med fördel genomföras parallellt med läsning av riktlinjerna i kapitel B – informationssäkerhet för medarbetare.

Klassning av informationsobjekt är en central del i kommunens arbete med informationssäkerhetsarbetet och finns med genomgående i dessa riktlinjer. Hur information klassas ska styra i vilken grad informationen ska skyddas. Klassningsmodellen är Sveriges kommuner och landstings verktyg KLASSA och den beskrivs i Kapitel A. KLASSA innehåller instruktioner hur information ska klassas och skyddas.

Riktlinjerna är baserade på den svenska och internationella standarden SS-ISO/IEC 27 002.

## Dispenser och undantag

Ansökan om dispenser från dessa riktlinjer ska ställas till kommunens informationssäkerhetsansvarige. Sådana ärenden ska beredas innan de ställs för att underlätta beslut. Exempelvis kan riskanalys ingå i beredning av ärendet. Beslut om godkännande av dispens ska fattas av kommunens informationssäkerhetsansvarige i samråd med berörda.

Undantag från riktlinjer för informationssäkerhet är inte permanenta utan ska ha en giltighetstid som bedöms från fall till fall. Efter det ska en ny begäran om dispens göras.  Bedömningen görs av informationssäkerhetsrådet under ledning av informationssäkerhetsansvarig.

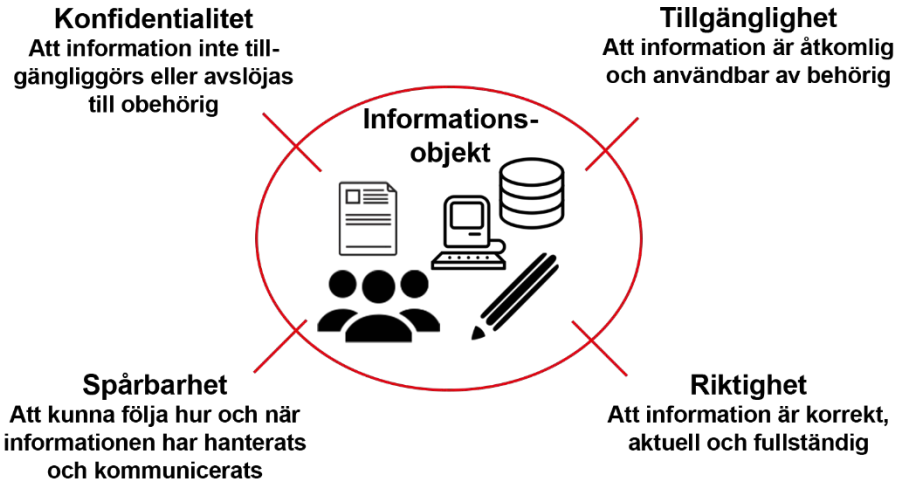
## Introduktion till informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former; text, ljud, bild, film osv. och oavsett hur information lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, papper eller direkt av oss människor i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-baserad informationshantering handlar informationssäkerhet alltså om all information, oavsett form. Detta inkluderar förutom information i IT-system även pappersbaserad information och om information som finns i våra huvuden.

Information är särskild/egen eller, aggregerad/samlad data som har ett värde för oss. Det är en tillgång som ska skyddas. Det finns flera fördelar och

gynnsamma effekter med en säker hantering av information. Rätt säkerhet innebär inte hög säkerhetsnivå, det innebär att hantera olika skyddsvärda informationsobjekt på rätt sätt.

Information och de resurser som används för att hantera information benämns informationsobjekt. Informationssäkerhet utgörs av fyra aspekter: Riktighet, konfidentialitet, spårbarhet och tillgänglighet (se Figur 1). Säkerhet handlar om att skapa strukturer och upprätthålla lämpliga rutiner och skydd av information. Det heter Ledningssystem för informationssäkerhet eller LIS.




Olika händelser (incidenter), som kan vara avsiktliga eller oavsiktliga, kan försämra konfidentialitet, spårbarhet, tillgänglighet eller riktighet hos informationsobjekt. Information kan på ett oönskat sätt t. ex. stjälas, raderas, förändras, eller göras otillgänglig.

En viss informationsmängd har krav på sig gällande de fyra aspekterna som kan vara interna eller härledas från rättsliga krav eller förväntningar och behov från externa aktörer. Rättsliga krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på en verksamhets informationshantering som ofta omfattar krav på informationens konfidentialitet, spårbarhet, tillgänglighet och riktighet. Dessutom har externa aktörer behov och förväntningar som påverkar organisationens informationssäkerhet.

Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbild, och i vilka situationer informationen hanteras – hur den lagras, bearbetas, kommuniceras osv.

## Informationssäkerhet och digitalisering

Digitalisering är en stor del av vardagen. I princip alla i samhället – privatpersoner, företag, myndigheter och andra organisationer – använder

datorer inom de flesta områden och till allt fler tjänster och datorerna är uppkopplade till ett gemensamt nätverk: Internet.

Möjligheterna är enorma med digitalisering och den alltmer utbredda användningen av internet skapar nya möjligheter att utföra tjänster och dela information. Dessa möjligheter (e-tjänster som bankärenden, inköp, bokningar, deklaration, omröstning) har lett till att de flesta idag förväntar sig att myndigheter, företag och andra organisationer ska erbjuda digitala tjänster på internet.

Det är inte bara traditionella datorer som är uppkopplade utan miljontals olika utrustningar, allt från kameror till bilar, kopplas upp mot internet (Internet of things). Digitaliseringen betraktas som en möjliggörare och motor för en utveckling som innebär nya förutsättningar för samhället och människan.

Säkert är att det för kommunal verksamhet innebär stora förändringar inom de flesta områden. Nya företeelser som e-hälsa, e-förvaltning. e-arkiv, e-demokrati, intelligenta transportsystem och smarta städer införs och digitalisering är redan något mer och samhällsomfattande än bara kommuners IT-drift. Denna förändring kommer att förändra mycket i grunden: vad vi gör, hur vi gör det och vad som går att göra. Information kommer att flöda i allt större mängder, genom och mellan organisationer, och till och från privatpersoner. Exempelvis kommer kommunens information att tillgängliggöras i högre grad genom individuellt anpassade digitala tjänster och service, förvaltningar kommer att göras mer transparenta, och medborgare kommer i högre grad att kunna föra dialog med beslutsfattare.

Tillsammans med digitaliseringens möjligheter finns också utmaningar och hot. Informationen är inte längre en organisations interna tillgångar och angelägenheter, utan flödar mellan organisationer i näringsliv och offentlig förvaltning, till och med mellan enskilda, och över nationsgränser. Gränser suddas ut mellan vem som äger och bär ansvar för viss information, vilket gör att det blir svårare att definiera hur den får användas och vem som kan och får ändra information, var ursprungsinformationen finns osv.

I och med att internet är en arena för hela samhället är det också en plats för samhällets baksidor. Virus och annan skadlig kod, bedrägerier, utpressning, stölder, näthat och förföljelser är företeelser som finns i olika former på nätet. Organiserad kriminalitet, extrema aktivistgrupper, terroristgrupper och stater har för länge sedan flyttat delar av sina verksamheter till internet. Det är idag enkelt att utföra destruktiva handlingar på nätet, de kan köpas på välorganiserade marknadsplatser där handel sker anonymt och krypterat. Löpande sker mängder av informationsrelaterade incidenter i Sverige och internationellt som beror på avsiktliga attacker såväl som misstag och olyckor.

Sammantaget innebär denna utveckling stora utmaningar för en kommuns informationssäkerhet. Information är en viktig och strategisk resurs som genomsyrar alla verksamheter. Utvecklingen där informationshantering och informationsflöden antar nya former i samhället, i kombination med en ökad och förändrad hotbild innebär att informationssäkerhet är en förutsättning för att Vårgårda kommun kan delta i det digitala samhället. En god informationssäkerhet möjliggör en tillförlitlig informationshantering och e-förvaltning med användning av ny teknik, men även befintlig teknik.

## Termer och definitioner

| Term | Definition |
|---|---|
| Autentisering | Verifiering av att en användare eller IT-resurs är den som den utger sig för at vara. |
| Behörighet | Tilldelade rättigheter att använda information eller en IT-resurs på ett specificerat sätt. |
| Data | Representation av fakta i form av t. ex. tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel. |
| Information | Innebörd av data, d. v. s. data tolkad av människor. |
| Informationssäkerhet | Konfidentialitet, spårbarhet, riktighet och tillgänglighet hos information. |
| Informationssäkerhetspolicy | Organisationens viljeinriktning med informationssäkerhet uttryckt av dess ledning. |
| Informationsobjekt | Information som är av värde för organisationen, och även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t. ex. rykte). |
| IT-resurs | IT-baserad komponent som hanterar information, t. ex. system, verktyg, tjänster och infrastruktur i form av mjuk- och/eller hårdvara. |
| IT-säkerhet | Säkerhet i IT-resurser för att uppnå och upprätthålla informationssäkerhet |
| Klassning | Att genom konsekvensanalys, identifiera skyddsbehovet för en viss informationsmängd. |
| Konfidentialitet | Att information inte tillgängliggörs eller avslöjas till obehörig |
| Ledningssystem för informationssäkerhet (LIS) | Ett administrativt ledningssystem som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. |
| Riktighet | Att information är korrekt, aktuell och fullständig. |
| Sekretess | Information som inte ska lämnas ut och bli allmänt tillgänglig. Sekretessbelagd uppgift innebär tystnadsplikt för den som har eller fått befattning om uppgiften. |
| Spårbarhet | Entydig härledning av utförda aktiviteter till en identifierad användare eller IT-resurs. |
| Tillgänglighet | Att information är åtkomlig och användbar av behörig. |

# Kapitel A: Styrning av informationssäkerhet

# Innehåll kapitel A

# Inledning

Detta kapitel beskriver och reglerar hur arbetet med informationssäkerhet ska bedrivas i Vårgårda kommun. Det beskriver också hur ansvarsfördelningen ser ut i stort. Ansvar för varje målgrupp återfinns också i varje kapitel, varför den övergripande ansvarsfördelningen i detta kapitel i huvudsak är informativ och ger en överblick över ansvaret för informationssäkerhet.

Den primära målgruppen för detta kapitel är de som arbetar med informations- och IT-säkerhet eller har ansvar för informationssäkerhet i informationsobjekt, projekt, processer eller andra verksamheter.

Kapitlet kan även vara informativt för andra som är intresserade av hur arbetet med informationssäkerhet bedrivs i Vårgårda kommun, exempelvis sådana som arbetar med ledning och styrning av andra närliggande områden och processer som exempelvis kvalitet och annan säkerhet.

## A1. Roller, ansvar och organisation

### Grundprincip

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Kommunens informationssäkerhetsansvarige och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor leder arbetet och fungerar som stöd till medarbetare, verksamheter och kommunens ledning.

### Övergripande ansvar

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet. Kommunfullmäktige fastställer övergripande mål och inriktning för informationssäkerhet genom en övergripande policy för informationssäkerhet.

Kommunchef har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunfullmäktiges fastställda policy för informationssäkerhet. Riktlinjer för informationssäkerhet fastställs av kommunstyrelsen.

Kommunledningen ansvarar för att alla medarbetare i Vårgårda kommun efterlever policy för informationssäkerhet och riktlinjer för informationssäkerhet. Kommunledningen bör visa sitt stöd för dessa dokument och fungera som förebild.

### Ansvar inom respektive verksamhet

Verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger ansvarig att se till att medarbetare

efterlever riktlinjer, har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att erforderlig informationssäkerhet i verksamheten kan uppnås. Lokala rutiner och anvisningar får beslutas om så länge de inte går emot centrala bestämmelser.

Säkerhetsansvaret kan inte delegeras, däremot kan ansvaret att genomföra viss arbetsuppgifter fördelas.

### Medarbetares ansvar

Alla medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler. Varje anställd har även skyldighet att rapportera informationssäkerhetsrelaterade brister och incidenter. Om någon enskild befattningshavare ändå bryter mot gällande styrdokument bär vederbörande själv ansvaret för sitt handlande.

### Personuppgiftsansvar

Kommunstyrelsen och nämnder är personuppgiftsansvariga inom respektive verksamhetsområde. Som personuppgiftsansvariga har de det yttersta ansvaret för all behandling av personuppgifter inom sitt verksamhetsområde. Om behandling sker i strid med Dataskyddsförordning eller andra bestämmelser kan den personuppgiftsansvarige ställas till ansvar, oavsett om denne haft uppsåt att handla i strid med lagen eller varit oaktsam.

### Objektsägaransvar

Objektsägare och/eller Systemägare ansvarar för att objekt och eller system efterlever policy för informationssäkerhet och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivåer genom klassning enligt verktyget KLASSA som tillhandahålls av Sveriges kommuner och landsting.
Informationssäkerhetsansvar hos övriga roller inom organisationen beskrivs i kapitel C.

I den mån det inte finns utpekade ägare, följer ansvaret verksamhetsansvaret.

### Ansvar i projekt

Verksamheten äger projektet via en utsedd projektägare som säkerställer att säkerhetsfrågorna beaktas. Styrgruppen är ansvarig för att säkerhetsfrågorna beaktas och ska tillsammans med projektägare fastställa säkerhetsnivån för det som utvecklas. Under projektets gång ska styrgruppen följa upp hanteringen av de säkerhetsrelaterade frågorna. Projektledaren ansvarar för att fastslagen säkerhetsnivå beaktas i projektarbetet.

### IT-avdelningens ansvar

IT-avdelningen ansvarar för att säkerheten i kommunens IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamhetens  krav, legala krav samt policy för informationssäkerhet och riktlinjer för informationssäkerhet.

### IT-säkerhetsansvarig

Det ska finnas en utpekad IT-säkerhetsansvarig som samordnar arbetet med säkerheten i Vårgårda kommuns IT-miljö och som är stödjande vid kravställning på externa aktörer. Rollen IT-säkerhetsansvarig beskrivs utförligare i Kapitel D.

### Informationssäkerhetsansvarig

Informationssäkerhetsarbetet i kommunen leds och samordnas av informationssäkerhetsansvarig. På delegation av kommunchef beslutar informationssäkerhetsrådet under ledning av informationssäkerhetsansvarig om godkännande av undantag i riktlinjer för informationssäkerhet i samråd med berörda samt kommunens säkerhetschef.

Informationssäkerhetsansvarig ansvarar för:

- Att kommunens styrande dokument inom området är aktuella
- Att utveckla och förvalta metoder, vägledningar och annat stödmaterial inom området
- Kompetensförsörjning och att öka medvetenheten inom kommunen t. ex. genom rådgivning och utbildning
- Att stödja verksamheterna i frågor som rör informationssäkerhet
- Kontroll och uppföljning av informationssäkerheten
- Omvärldsbevakning inom informationssäkerhetsområdet
- Leda kommunens informationssäkerhetsråd (se nedan)

### Informationssäkerhetsrådet

Leds av informationssäkerhetsansvarig som adjungerar övriga ledamöter, vid behov även kommunens säkerhetschef. Informationssäkerhetsrådet ska sammanträda fyra gånger per år och har uppgift och befogenhet att:

- Bereda och registrera ärenden som gäller undantag från kommunens riktlinjer för informationssäkerhet
- Bereda dokument, t. ex. styrande dokument, metoder och vägledningar
- Fungera som remissinstans och rådgivare i relaterade frågor
- Vara ett forum för erfarenhetsutbyte och omvärldsbevakning
- Godkänna specifika säkerhetslösningar som t. ex. krypteringsmetoder

## A2. Dokumentstruktur

De dokument som är centrala för kommunens arbete med informationssäkerhet:

- Policy för informationssäkerhet
- Riktlinjer för informationssäkerhet
- Analys för informationssäkerhet – Tas fram av ansvarig efter en genomlysning
- Handlingsplan för informationssäkerhet – Tas fram årligen och innehåller mål och åtgärder baserade på analysen för informationssäkerhet.

Policy för informationssäkerhet och Riktlinjer för informationssäkerhet riktar sig till alla medarbetare i Vårgårda kommun.

Analys och handlingsplan riktar sig främst till de som arbetar med styrning av informationssäkerhet i Vårgårda kommun.

Modeller, metoder, vägledningar och andra stöddokument kan tas fram centralt för att stödja arbetet med informationssäkerhet på olika nivåer och att underlätta tillämpningen efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet.

Lokalt, t.ex. i verksamheter och IT, kan mer specifika anvisningar och guider tas fram i syfte att komplettera eller förtydliga riktlinjerna för informationssäkerhet.

| **Riktlinjer för dokumentstruktur för informationssäkerhet** | |
|---|---|
| A.2.1 | Vårgårda kommuns informationssäkerhet och dess behov ska analyseras i en informationssäkerhetsanalys. Analysen ska genomföras minst vart fjärde år och ska ligga till grund för hur arbetet med informationssäkerhet ska bedrivas och innehåll och utformning av övriga styrande dokument. |
| A.2.2 | Årliga handlingsplaner för informationssäkerhet ska tas fram baserade på informationssäkerhetsanalyser. |
| A.2.3 | Det ska finnas en för Vårgårda kommun övergripande informationssäkerhetspolicy som uttrycker ledningens viljeinriktning med informationssäkerhet. |
| A.2.4 | Det ska finnas kommunövergripande riktlinjer för informationssäkerhet som konkretiserar informationssäkerhetspolicyn och som riktar sig till relevanta målgrupper. |
| A.2.5 | Det ska finnas modeller, metoder, vägledningar och andra stöddokument som stödjer olika gruppers efterlevnad av informationssäkerhetpolicyn och riktlinjerna för informationssäkerhet. |

## A3. Informationsklassning

Informationsklassning är en grundläggande komponent i arbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet, tillgänglighet och spårbarhet skapar man förståelse för, och kan styra vilket skydd som krävs för olika informationsmängder. Främst handlar det om att skyddet ska bli tillräckligt, men ibland också för att undvika överskydd – med onödigt höga kostnader som följd. Klassning av information ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Vårgårda kommun.

Att klassificera information på ett enhetligt sätt utifrån konfidentialitet, riktighet, tillgänglighet och spårbarhet grunden i ett ledningssystem för informationssäkerhet (LIS) och ett krav i standarden SS-ISO/IEC 27001, vilken Vårgårda kommun ska arbeta enligt. Det är också en rekommendation från Myndigheten för samhällsskydd och beredskap att organisationer ska klassa information och bygga säkerhetsåtgärder utifrån resultatet.

| **Konsekvensnivå** ***Skyddsbehov*** | **Tillgänglighet** | **Konfidentialitet** | **Riktighet** |
|---|---|---|---|
| **Allvarlig** ***Hög skyddsnivå*** | Information där förlust av tillgänglighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av konfidentialitet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av riktighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. |
| **Betydande** ***Utökad skyddsnivå*** | Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av riktighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. |
| **Måttlig** ***Grundläggande skyddsnivå*** | Information där förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. |
| **Ingen** ***Ingen skyddsnivå*** | Förlust av tillgänglighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av konfidentialitet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. | Information där förlust av riktighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. |

## A4. Ledningssystem för informationssäkerhet

I Vårgårda kommuns informationssäkerhetspolicy anges att man ska bedriva ett systematiskt informationssäkerhetsarbete som baseras på standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).

Ett LIS är ett etablerat begrepp för ett systematiskt arbete med informationssäkerhet och innebär en metodik som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. LIS avser här inte ett IT-baserat system, även om IT-stöd kan användas i delar av ett LIS.

Eftersom kommunen och dess omvärld är i ständig förändring är informationssäkerhetsbehovet dynamiskt och måste ständigt anpassas till exempelvis organisationsförändringar, nya lagar, nya hotbilder och strömningar i samhället. Det räcker därför inte att skapa ett skydd som svarar mot interna och externa förutsättningar idag, eftersom dessa kan se annorlunda ut i morgon.

Ett systematiskt arbete med informationssäkerhet med ett LIS syftar i stort till att informationssäkerheten över tid anpassas efter interna och externa förutsättningar, och som därigenom upprätthåller en lämplig skyddsnivå över tid.

Som anges i informationssäkerhetspolicyn ska Vårgårda kommuns LIS utgå från standardserien SS-ISO/IEC 27000. Standardserien innefattar en stor mängd standarder, men två standarder kan sägas utgöra seriens huvudstandarder:

- **SS-ISO/IEC 27001:2017 – Informationsteknik – Säkerhetstekniker Ledningssystem för informationssäkerhet – krav.** Denna standard ställer som namnet antyder krav på ett LIS, dvs. vad det ska innefatta. I standardens bilaga B finns ett antal säkerhetsåtgärder som tjänar som utgångspunkt för vilka säkerhetsåtgärder som ska finnas.
- **SS-ISO/IEC 27002:2017 – Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder.** Denna standard ger vägledning för införande av säkerhetsåtgärderna i föregående standards bilaga B.

Standarderna i serien utgår från ett verksamhetsdrivet och riskorienterat arbete med informationssäkerhet, i motsats till ett teknikdrivet. Utgångspunkten är också att det är information som ska skyddas, utifrån de fyra aspekterna spårbarhet, konfidentialitet, riktighet och tillgänglighet, medan IT är sekundära resurser som används för att hantera informationen.

Att standardserien är så etablerad och spridd innebär fördelar. Förutom att man tar tillvara samlade kunskaper och erfarenheter från hela världen så använder man ett gemensamt ramverk och en gemensam terminologi som underlättar vid kommunikation och samverkan med andra aktörer, exempelvis i samband med utbildning, revisioner och upphandlingar.

| **Riktlinjer för ledningssystem för informationssäkerhet (LIS)** | |
|---|---|
| A.4.1 | Vårgårda kommun ska arbeta enligt ett ledningssystem för informationssäkerhet. (LIS) |

## A5. Personalsäkerhet

Personal är den viktigaste resursen i kommunen, och det är personal som dagligen hanterar information, manuellt eller med stöd av IT. Många roller kommer i kontakt med och hanterar kritisk och känslig information, och det är därför att av största vikt att personalen får information och utbildning om informationssäkerhet, och att det finns rutiner i samband med anställning, förändring och avslut av anställning.

### Före och i samband med anställning

Bakgrundskontroll av sökande till tjänster i Vårgårda kommun ska ske genom verifiering av sökandes meritförteckning, t.ex. genom kontakt med referenser och bekräftelse av akademiska och yrkesmässiga kvalifikationer.

För vissa kritiska tjänster krävs en förstärkt kontroll form av kreditupplysning och kontroll i brottsregister. Sådana kritiska tjänster är högre chefstjänster, säkerhetstjänster, eller för de som har åtkomst till känslig eller samhällsviktig information.

För befattningar som har betydelse för rikets säkerhet, och således omfattas av Säkerhetsskyddslagen (1996:627), ska det i anställningsförfarandet genomföras en registerkontroll. Registerkontrollen ska genomföras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. De befattningar som är aktuella framgår av Vårgårda kommuns säkerhetsskyddsplan.

Alla bakgrundskontroller ska ta hänsyn till gällande lagstiftning rörande hantering av personuppgifter.

Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. Delgivning och utbildning ska också ges kopplat till annat ansvar som följer med rollen, t.ex. informationsägarskap. Alla anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal som även ska gälla efter avslut av anställning.

| **Riktlinjer för personalsäkerhet före och i samband med anställning** | |
|---|---|
| A.5.1 | Bakgrundskontroll av sökande ska göras före anställning där sökandes meritförteckning verifieras. |
| A.5.2 | Anställning av kritiska roller ska genomgå förstärkt kontroll i form av kreditupplysning och kontroll i brottsregister. |
| A.5.3 | För befattningar som har betydelse för rikets säkerhet, och som omfattas av Säkerhetsskyddslagen (1996:627) ska det i anställningsförfarandet genomföras en registerkontroll. |
| A.5.4 | Nyanställda ska delges ansvar och skyldigheter kopplade till informationssäkerhet och genomgå utbildning i informationssäkerhet samt ta del av informationssäkerhet för medarbetare enligt dessa riktlinjer. och annat ansvar som följer med rollen, t.ex. informationsägarskap |
| A.5.5 | Anställda som får tillgång till konfidentiell information ska underteckna ett sekretessavtal. |

## A6. Leverantörsrelationer

Utfallet av informationsklassning i SKL:s verktyg KLASSA ska tas hänsyn till vid extern upphandling. Den ska kunna användas som stöd vid extern upphandling av IT-tjänster såsom system och molntjänster.

| **Riktlinjer för leverantörsrelationer** | |
|---|---|
| A.6.1 | Det ska finnas en vägledning med informationssäkerhetskrav som ska baseras på Vårgårda kommuns informationsklassning (KLASSA).. |

## A7. Efterlevnad och granskning

Efterlevnad av de styrande dokumenten Informationssäkerhetspolicy och Riktlinjer för informationssäkerhet ska följas upp. I praktiken innebär det främst att riktlinjerna för informationssäkerhet granskas och följs upp; att riktlinjerna efterlevs och att säkerhetsåtgärder införs och får avsedd verkan. I synnerhet gäller detta de särskilda säkerhetsåtgärder som gäller för information, objekt och IT-resurser med höga skyddskrav.

Granskning och uppföljning av informationssäkerhet, inklusive dess styrning utförs genom ledningssystem för informationssäkerhet (LIS).

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. systemförvaltarplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet.

Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Detta regleras av riktlinjer i Kapitel D – Informationssäkerhet i IT-miljön (avsnitt D10).

| **Riktlinjer för efterlevnad och granskning av informationssäkerhet** | |
|---|---|
| A.7.1 | Efterlevnaden av informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet ska följas upp. |
| A.7.2 | Vårgårda kommuns informationssäkerhet ska granskas och utvärderas årligen. |

B

# Kapitel B: Medarbetare

# Inledning

Detta kapitel vänder sig till alla medarbetare vid Vårgårda kommun. Riktlinjerna gäller även extern personal som har åtkomst till Vårgårda kommuns information, exempelvis inhyrda konsulter.

Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Vårgårda kommun och vilka regler som gäller.

Vårgårda kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

Informationssäkerhet för medarbetare följer i stort en struktur framtagen av Myndigheten för samhällsskydd och beredskap – MSB – som finns i en utbildning för informationssäkerhet: DISA (Datorstödd Informationssäkerhetsutbildning för användare).

Syftet är att anställda kan genomgå DISA-utbildningen och parallellt se vilka riktlinjer som gäller i Vårgårda kommun.

DISA består av 10 avsnitt om informationssäkerhet, och alla avsnitt utgörs av en film med tillhörande information och frågor. Dessa riktlinjer består dock endast av åtta avsnitt (A1 – A8), eftersom information och regler gällande mobila enheter, smarta telefoner och surfplattor slagits samman till ett avsnitt (avsnitt A2).

## Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Vårgårda kommun och är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör t.ex. förskolor, grundskolor, gymnasium, socialtjänst, hemvård, stadsplanering och bygglov. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av texter, men även bilder, symboler, filmer och ljud utgör information.

Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada. Det finns en hel del lagar och föreskrifter som kommunen måste leva upp till, och privatpersoner, företag och andra har förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav.

Information behöver olika former av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, eller administrativt i form av regler (som dessa riktlinjer) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp m.m. Även medarbetares kunskap och medvetenhet är ett viktigt skydd, t.ex. att arbeta på rätt sätt med pappersdokument och i IT-system och att vara

försiktig med känslig information som t.ex. personuppgifter. Säkerhet är inte bättre än den svagaste länken, och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av Vårgårda kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Vårgårda kommun ställer krav på att medarbetare följer dessa riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare.

Om du som medarbetare eller externt kontrakterad har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att anställningen eller avtalet upphört.

Vid underlåtenhet att följa dessa riktlinjer för informationssäkerhet följer Vårgårda kommun reglerna enligt lagar och avtal. Lagbrott polisanmäls.

### Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på Vårgårda kommuns information. Det kan röra sig om t.ex.

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Brister i efterlevnad av dessa riktlinjer för informationssäkerhet

IT- och informationsrelaterade incidenter och brister ska rapporteras till närmaste chef. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga, ska inte själva försöka bevisa sådana då det kan försvåra framtida utredningar.

## B1. Lösenord

För att logga in till de flesta av Vårgårda kommuns IT-system används användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn.

Via Vårgårda kommuns lösenordsportal blir du påmind om när lösenord behöver bytas och kan få ett nytt om du har glömt ditt lösenord.

Användar-ID och lösenord används för att skydda information som kan vara intern eller **konfidentiell**, och det är därför viktigt att följa nedanstående regler för skapande och hantering av lösenord.

Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet.

| **Riktlinjer för utformning av lösenord** | |
|---|---|
| B.1.1 | Lösenord ska vara minst 8 tecken långt, gärna längre. |

| | |
|---|---|
| B.1.2 | Lösenord ska innehålla minst en gemen, en versal och en siffra. Siffra ska inte stå i början eller slut. |

Användar-ID och lösenord är i sig viktig information där Användar-ID är intern information medan lösenord är konfidentiell information och ska hanteras på ett säkert sätt.

| **Riktlinjer för hantering av lösenord** | |
|---|---|
| B.1.3 | Lösenord ska inte vara synliga. Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet. |
| B.1.4 | Olika lösenord ska användas. Samma lösenord ska inte användas privat och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information. |
| B.1.5 | Lösenord ska bytas regelbundet. Lösenordsportalen tvingar fram byte av lösenord var 90:e dag. Om man arbetar i system där lösenordsbyte inte är tvingande, ska man ändå byta ut lösenordet några gånger om året. Lösenord ska bytas direkt om misstanke finns att det har röjts. |
| B.1.6 | Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen. |
| B.1.7 | Automatisk minnesfunktion för lösenordet ska inte användas. Om man loggar in på webbsidor så ska man inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. Detta är särskilt viktigt då en dator delas av flera. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/ta bort lösenord, vilken kan användas om man är osäker på om lösenord har lagrats. |

## B2. Mobila enheter

Den IT-utrustning som tillhandahålls av Vårgårda kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Mobil enhet avser bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta.
Applikationsspecifika datorer, mobiler eller surfplattor som exempelvis TES-mobiler, kan ha specifika riktlinjer utöver dessa som presenteras här. Kolla med din chef om du är osäker vad som gäller.

| **Riktlinjer för hantering av mobila enheter** | |
|---|---|
| B.2.1 | Mobila enheter som tillhandahålls av Vårgårda kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera. |
| B.2.2 | Uppsatta säkerhetsinställningar i enheter får inte ändras. |
| B.2.3 | Endast godkända programvaror får installeras på enheten. |
| B.2.4 | Installerad programvara får inte kopieras eller installeras på annan enhet. |
| B.2.5 | Mobila enheter ska låsas med lösenord. |
| B.2.6 | Konfidentiell information måste vara krypterad på mobila enheter. |
| B.2.7 | Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras. |
| B.2.8 | Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät. |
| B.2.9 | Privat utrustning kan anslutas till kommunens gästnät. |
| B.2.10 | Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade. |

| | |
|---|---|
| B.2.11 | Vid distansarbete måste godkänd säker utrustning och anslutning användas. |

| **Riktlinjer för fysisk hantering av mobila enheter.** | |
|---|---|
| B.2.12 | Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd. |
| B.2.13 | Arbete med konfidentiell information får inte ske i publika miljöer. |
| B.2.14 | Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme. |
| B.2.15 | Förlust av enhet ska omedelbart anmälas till Servicedesk, detta ska göras innan polisanmälan. I vissa fall finns möjligheter att fjärradera information. |
| B.2.16 | Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat eller av en verksamhet. |
| B.2.17 | Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, t.ex. skyddas mot värme och fukt. |

Särskilda regler för smarta telefoner och surfplattor

Förutom de regler som gäller allmänt för mobila enheter gäller även följande vid användning av smarta telefoner och surfplattor:

| **Riktlinjer för**<br>**Regler för smarta telefoner och surfplattor** | |
|---|---|
| B.2.18 | Vårgårda kommun är som arbetsgivare ägare till de smarta telefoner och surfplattor som används i tjänsten och även till den information som finns i dessa. Man bör därför som medarbetare vara medveten om att arbetsgivaren har rätt att ta del av t.ex. sms, foton och kalenderanteckningar. Eftersom offentlighetsprincipen gäller kan det vara möjligt för utomstående att begära ut informationen. |
| B.2.19 | Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. I syfte att minska denna risk är det endast tillåtet att ladda ned appar från Vårgårda kommuns interna appkatalog, App Store eller Google Play. |
| B.2.20 | Information som är konfidentiell får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används. |
| B.2.21 | Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc. användas, och inte samma pinkod som används i andra sammanhang, t.ex. pinkod till bankomatkort. |
| B.2.22 | Vårda utrustningen och använd exempelvis skärmskydd och skal. |

## B3. Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke, och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

Skadlig kod är ett växande problem och den blir mer och mer sofistikerad och ”intelligent” och kan vara svår att upptäcka och kan utföra avancerade operationer. Man behöver idag inte vara en teknisk kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på Internet.

Exempel på idag förekommande skadlig kod:

- Vissa trojaner, s k keyloggers, kan avlyssna lösenord och skicka dessa vidare.
- Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap. Exempelvis med syfte att lagra olaglig information.
- Ett ökande problem är s k Ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma.

### Spridning av skadlig kod

Skadlig kod kan spridas till en dator eller mobila enhet om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier.

Avsändare till e-post kan fejkas och webbsidor är inte alltid de som de utger sig för att vara. Identiteter kan kapas, t.ex. på Facebook, och e-postadresser kan förfalskas i syfte att lura mottagaren att klicka på länkar. Vid s k Phishing luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fylla aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt.

IT-utrustning som drabbats av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada.

Kommunens datorer är utrustade med skydd mot skadlig kod. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

| **Riktlinjer för skydd mot skadlig kod** | |
|---|---|
| B.3.1 | Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod. |
| B.3.2 | Anslut endast godkänd IT-utrustning till kommunens nätverk. |
| B.3.3 | Var misstänksam och undvik att klicka på konstiga länkar eller fyll i irrelevanta uppgifter. |
| B.3.4 | Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. |
| B.3.5 | Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta Kommunsupporten. |

## B4. Internet och sociala medier

Förutom de riktlinjer som är kopplade till skadlig kod i avsnitt B3 finns här särskilda regler för användning av Internet och sociala medier.

| **Riktlinjer för Internetanvändning** | |
|---|---|
| B.4.1 | Internet används som ett arbetsverktyg av medarbetare i Vårgårda kommun och är främst ett arbetsverktyg och annat användande ska |

| | |
|---|---|
| | inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen. |
| B.4.2 | De regler som gäller i samhället i övrigt gäller självklart även inom Vårgårda kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som även måste beaktas när man använder Internet. |
| B.4.3 | För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren. |
| B.4.4 | I begränsad omfattning får Internet användas för privata syften. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Vårgårda kommuns nätverk. |
| B.4.5 | Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller konfidentiell information. |

Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstepersonen som utför aktiviteten, och även för Vårgårda kommun som organisation. Det är därför särskilt viktigt att som representant för Vårgårda kommun beakta god etik och gott omdöme på Internet. Vårgårda kommuns värdegrund ska följas även vid kommunikation via Internet och sociala medier. Tänk därför på att:

| **Etiska riktlinjer** | |
|---|---|
| B.4.6 | All kommunikation på Internet från Vårgårda kommuns datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker för privata syften eller inte. |
| B.4.7 | Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll. |
| B.4.8 | Publicera inte något på Internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt samt finns kvar under lång tid. Tänk därför igenom innehållet noga innan du publicerar. |

Vårgårda kommun är aktiv på sociala medier. Den personal som skriver i Vårgårda kommuns namn har särskilda regler och kunskap om kommunikation. Tänk på följande:

| **Riktlinjer vid användning av sociala medier** | |
|---|---|
| B.4.9 | Vid privat användning av sociala medier, se till så att det inte framstår som om åsikter som uttrycks är Vårgårda kommuns. |
| B.4.10 | Även då du använder sociala medier privat, så kan kopplingar göras till din arbetsgivare. |
| B.4.11 | Utgå från Vårgårda kommuns Riktlinjer för Sociala medier |

## B5. E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med e-post normalt är helt öppen. Att sända e-post som inte är skyddad, t.ex. med kryptering, kan jämföras med att skicka vykort.

| | |
|---|---|
| **Ansvar** | |
| B.5.1 | Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot. |
| B.5.2 | Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post. Vid frånvaro, t.ex. semester, sjukfrånvaro eller föräldraledighet, ska autosvar användas, och om nödvändigt hänvisning till kollega eller chef. Vid avslut av anställning eller vid tjänstledighet tas e-posten bort. |
| B.5.3 | E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga. |
| **Allmänna handlingar** | |
| B.5.4 | E-post som skickas till personliga brevlådor är allmän handling om innehållet är arbetsrelaterat. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas. Huvudregeln är att e-post som är allmän handling omgående ska hanteras som sådan. |
| B.5.5 | E-post som är allmän handling får gallras, dvs. raderas, först när e-posten diarieförts. Vissa e-postmeddelanden som är allmänna handlingar är av uppenbar ringa eller tillfällig betydelse och är undantagna från kravet på registrering. Dessa får gallras efter en vecka. |
| **Privat e-post** | |
| B.5.6 | Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd restriktivt ditt e-postkonto i Vårgårda kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsmaterial. |
| B.5.7 | Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser. |
| **E-post och konfidentiell information** | |
| B.5.8 | Öppen och intern information får skickas med e-post, medan konfidentiell information endast får skickas med e-post som använder av Vårgårda kommun godkänd kryptering. |
| B.5.9 | Dokument som skannas skickas ofta med e-post från skannern till mottagarens e-postadress. Skanning av dokument som innehåller konfidentiell information ska även den krypteras av Vårgårda kommun godkänd kryptering. |

## B6. Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av diskkrasch, oavsiktlig radering m.m.

| | |
|---|---|
| **Riktlinjer för lagring och säkerhetskopiering** | |
| B.6.1 | Information ska lagras på nätverket så att den säkerhetskopieras. Det kan vara personliga (H:) eller gemensamma filareor (K:). |
| B.6.2 | Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket. |
| B.6.3 | Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska Servicedesk kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian. |
| B.6.4 | Konfidentiell information får endast lagras i därför avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan. |
| B.6.5 | Lokal lagring av konfidentiell information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Vårgårda kommun godkänd metod för kryptering. |
| B.6.6 | Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta. |

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror.

| Riktlinjer för lagring i molntjänster | |
|---|---|
| B.6.7 | Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet. |
| B.6.8 | Konfidentiell information får inte lagras i molntjänster. |

## B7. Spårbarhet och loggning

Loggning sker i kommunens system, datorer och nätverk och innebär att uppgifter om vem som gjorde vad, och när, sparas. Det gäller både de åtgärder som användaren vidtar, samt de åtgärder som systemet vidtar automatiskt när användaren arbetar med datorn. Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. Loggarna lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer.

Spårbarhet innebär i det här sammanhanget att man genom loggning kan identifiera och följa förloppet för olika händelser som skett på datorn. Syftet är att finna vem som är skyldig till ett intrång eller en säkerhetsrelaterad incident. Manipulation av loggar är för övrigt ett vanligt sätt att försöka dölja intrång och bedrägeri på.

All Internettrafik och e-post loggas centralt. Vårgårda kommun har som arbetsgivare rätt att gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning, riktlinjer, felsökningar eller vid annan utredning av skada (eller hot). Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

| Information om genomgång av loggar | |
|---|---|
| B.7.1 | Närmsta chef ansvarar för att meddela medarbetare som blir föremål för utredning av hans eller hennes loggar för internettrafik och e-post. |

## B8. Konfidentialitet och säkert beteende

En stor del av kommunens information hanteras muntligt, elektroniskt eller på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar konfidentiell information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara t.ex. omdömen om chefer och medarbetare – skvaller, rykten m.m. – eller information om en oförutsedd händelse, t.ex. ett brott. Sådan information kan vara känslig och är i så fall konfidentiell information.

| Riktlinjer för muntlig information | |
|---|---|
| B.8.1 | Konfidentiell information har en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer men även i informella sammanhang, t.ex. vid fikabordet. |
| B.8.2 | Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön. Konfidentiell information får överhuvudtaget inte kommuniceras muntligt i publika lokaler. |
| **Riktlinjer för information på skärmar och i pappersform** | |

| | |
|---|---|
| B.8.3 | Skriftligt material som innehåller konfidentiell information får inte ligga framme så att obehöriga kan ta del av den. Materialet ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder. |
| B.8.4 | Konfidentiell information på datorskärmen eller mobila enheter ska vara skyddade från obehöriga. Enheten ska låsas när man lämnar den, även för en kortare stund. Om man har ett s k smart kort till datorn ska detta tas ut då man lämnar arbetsplatsen. |
| B.8.5 | Besökare får inte vistas utan uppsikt i lokaler där konfidentiell information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta. |
| B.8.6 | Vid fysisk posttjänst ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller konfidentiell information. |
| B.8.7 | Då konfidentiell information överförs via fax ska man försäkra sig om att man har rätt nummer (t.ex. använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar. |
| B.8.8 | Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av konfidentiell information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen. |
| B.8.9 | Pappersdokument som innehåller konfidentiell information måste vid gallring strimlas eller kastas i godkända säkerhetskärl. |

C

# Kapitel C: Informationssäkerhet i verksamhet och förvaltning

# Inledning

Vårgårda kommun har beslutat att arbeta utifrån ett ledningssystem för informationssäkerhet (LIS). I kommunens policy för informationssäkerhet och personuppgiftshantering finns ett antal principer som gäller för detta. Det här kapitlet konkretiserar den policyn med särskilda riktlinjer rörande informationssäkerhet.

För varje system eller objekt ska det upprättas en systemförvaltningsplan för att säkerställa drift och tillämpning av riktlinjerna för informationssäkerhet. Det ska finnas en utsedd ägare för varje system som ansvarar för säkerheten i systemet. De riktlinjer som finns i detta kapitel gäller även för dessa personer.

## Roller och ansvar

Nedan beskrivs ansvar rörande informationssäkerhet för rollerna i den verksamhetsnära förvaltningen. Motsvarande ansvar för de IT-nära rollerna återfinns i Kapitel D – informationssäkerhet i IT-miljön.

Ansvaret för informationssäkerhet följer verksamhetsansvaret, från kommunledningen till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Den av kommunen utsedde informationssäkerhetsanvarige och övriga som jobbar specifikt med informationssäkerhet fungerar som stöd till kommunens verksamheter att uppfylla informationssäkerhetsansvaret. Informationssäkerhetsansvariges roll och ansvar beskrivs i kapitel A. Roller och ansvar i den verksamhetsnära förvaltningen beskrivs nedan:

**Ledning**, i form av kommunfullmäktige, kommunstyrelse och nämnder har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom respektive ansvarsområde.

**Verksamhetschef** ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetschef ansvarar också för att medarbetare inom den egna verksamheten har ett säkerhetsmedvetande samt tillräcklig kunskap och förståelse för att nödvändig informationssäkerhet i verksamheten ska uppnås.

**System- eller objektägare** ansvarar för att informationsobjekt efterlever policy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om tillgångens säkerhetsnivåer genom informationsklassning. System- eller objektägaren ansvarar också för att upprätta systemförvaltningsplaner.

**Systemförvaltare**, ansvarar för att tillsammans med systemägaren upprätta systemförvaltningsplan och säkerställa efterlevnaden av upprättad plan. Det senare handlar bland annat om att informationssäkerhetsrelaterade mål och åtgärder nås respektive genomförs.

## C1. Dokumentation av informationssäkerhet

Informationssäkerhet ska vara en naturlig del i förvaltningen av objekt och system kommunen använder. Säkerhetsförhållanden ska vara dokumenterade i systemförvaltningsplanen.

Genom att klassa system i SKL:s verktyg KLASSA och upprätta systemförvaltningsplaner framkommer nödvändiga handlingsplaner och säkerhetsmål. Mål och åtgärder kan dessutom uppkomma eller motiveras med exempelvis resultat från riskanalyser och revisioner, erfarenheter från inträffade incidenter eller krav i dessa riktlinjer.

| **Informationssäkerhet i systemförvaltningsplaner** | |
|---|---|
| C.1.1 | Systemförvaltningsplaner ska upprättas för varje system |
| C.1.2 | Nödvändiga system och objekt ska klassas. |

### Systemsäkerhetsbeskrivning

Säkerhetsförhållanden ska dokumenteras i KLASSA och resultatet ska ligga till grund för en så kallad systemsäkerhetsbeskrivning i systemförvaltningsplanen. Av systemsäkerhetsbeskrivningen ska framgå:

- Vilka informationsmängder som hanteras i systemet och hur dessa är klassade (se avsnitt C2).
- Hur systemet är klassat (se avsnitt C2).
- Hur behörighetshantering och loggning går till (se avsnitt C3).
- Hur ändringshantering går till (se avsnitt C4).
- Användarinstruktioner med inriktning på säkerhet (se avsnitt C5).
- Planerade och genomförda riskanalyser och resultat från dessa (se avsnitt C6).
- Hur incidenthantering går till och vilka incidenter som har inträffat med referenser till incidentrapporter (se avsnitt C7).
- Vilken kontinuitetshantering som finns (se avsnitt C8).

| **Objektsbeskrivning** | |
|---|---|
| C.1.3 | System ska ha en systemsäkerhetsbeskrivning i systemförvaltningsplanen där systemets informationssäkerhet är dokumenterad. |

## C2. Informationsklassning och systemklassning

Informationsklassning innebär att information klassas i olika nivåer utifrån dess skyddskrav. Genom att klassa information på detta sätt kan man identifiera känslig och kritisk information så att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd med höga kostnader som följd. System ska också klassas och den klassningen ska baseras på hur den ingående informationen är klassad. Klassning av information och system ska ske i enlighet med SKL:s modell för informationsklassning som beskrivs i Kapitel A.

Informationsklassning ska ske utifrån rättsliga krav som lagar och föreskrifter, men även interna krav på informationens värde, känslighet och betydelse för Vårgårda kommuns verksamheter.

Frågor man ska ställa sig när man klassar är:

- Vilka konsekvenser blir det om informationen läcker till obehöriga (konfidentialitet)?
- Vilka konsekvenser blir det om informationen är felaktig eller inaktuell (riktighet)?
- Vilka konsekvenser blir det om (behöriga) inte får tillgång till informationen (tillgänglighet)?
- Vilka konsekvenser blir det om genomförda åtgärder i ett system inte kan härledas till enskilda användare (spårbarhet)?

KLASSA ska identifiera verksamhetens behov av tekniska och administrativa säkerhets- och skyddsåtgärder för informationen. Verktyget används för att värdera informationen i kommunens system och genererar handlingsplaner som identifierar en del av de åtgärder som behöver vidtas för att uppfylla beslutad säkerhetsnivå.. Givetvis kan det dock krävas fler åtgärder utifrån andra överväganden och behov som inte KLASSA omfattar, som t.ex. interna och avtalsmässiga krav.

Särskilda rutiner och regler ska upprättas för hantering av konfidentiell information, som exempelvis skyddade personuppgifter. Sådana rutiner och regler ska finnas med i användarinstruktioner (se avsnitt C5).

| **Riktlinjer för klassning av system och objekt** | |
|---|---|
| C.1.3 | Data eller information i system ska vara inventerad och klassad enligt SKL:s modell för informationsklassning. |

## C3. Behörighetshantering och loggning

Behörigheter innebär vissa rättigheter att använda informationsobjekt, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

För att skydda information mot obehörig åtkomst behöver användare ange en identitet som kan verifieras (autentiseras), vanligen med användar-ID och lösenord. Ju känsligare information som bearbetas, desto högre är kravet på skydd mot obehörig åtkomst.

### Behörighetstilldelning

Grundprincipen för behörighet ska baseras på vilken information användare behöver för att kunna utföra sina arbetsuppgifter. Olika roller som använder ett system kan ha olika behov av information och ska därför ha olika typer av behörigheter eller s.k. åtkomstprofiler. En förutsättning för rätt

behörighetstilldelning är att informationen är strukturerad och klassad så att rätt åtkomstregler kan upprättas.

### Behörighetstilldelning inom vård och omsorg m.m.

Inom vissa områden, som t.ex. vård och omsorg, behöver man ha (teknisk) behörighet till en stor mängd information. I akuta situationer måste kanske annan vårdande personal än den ordinarie ha åtkomst till patientinformation. Här behövs istället regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. Sådan åtkomstkontroll måste kompletteras med funktioner för uppföljning, övervakning och loggning. Detta kan – och ska – påverka användarna så att dessa avhåller sig från otillåtna men tekniskt möjliga operationer i ett system.

### Ansvar för behörighetstilldelning

Systemägare bestämmer vilka som ska få tillgång till system som ingår i objekt och vilka behörigheter dessa ska ha. Verksamhetens art och dess krav på informationens konfidentialitet och riktighet, tillsammans med legala krav som lagar, föreskrifter och avtal, styr hur behörigheterna ska se ut.

För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomsttilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

Varje användare ska ha ett unikt Användar-ID, dvs. gruppidentiteter är inte tillåtna (under vissa förutsättningar kan dock detta beviljas, se information under D.2.14).

### Process eller rutiner för behörighetsförvaltning och revision

Det ska finnas en process eller rutiner som underhåller och förvaltar behörigheter för ett system, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst.

Sådana processer eller rutiner måste vara kopplade till IT-avdelningen så att tekniska förändringar genomförs. Objektägare IT ska säkerställa den del av rutinen som rör införande, förändring samt borttagning av åtkomst i IT-resurser. I Kapitel D finns riktlinjer för hur åtkomstkontroll ska ske i IT-miljön (avsnitt D2 – Styrning av åtkomst). Exempelvis ska stark autentisering finnas för åtkomst till system som innehåller information med **höga skyddskrav** avseende konfidentialitet och riktighet.

Vid anställning eller förändring av roll samt vid upphörande av anställning ska rapportering göras omedelbart till personalavdelningen så att reglering av behörigheter kan ske.
Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

### Logghantering

För att erhålla spårbarhet och att exempelvis möjliggöra incidentutredningar samt för att upptäcka avvikelser från legala eller interna regelverk bör system övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Detta är särskilt viktigt, och obligatoriskt, om system hanterar information med **höga skyddskrav** eller om regelstyrd behörighetshantering används istället för teknisk dito.

Då loggning används ska det finnas processer eller rutiner för dess hantering. Sådana ska innefatta hur loggning går till, hur loggar skyddas mot manipulation och obehörig åtkomst, hur länge de sparas och hur de granskas. I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av dataskyddsförordningen. Detta innebär bland annat att om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke.

Processer och rutiner för loggning ska följas upp och dokumenteras.

| **Riktlinjer för behörighetshantering och loggning** | |
|---|---|
| C.3.1 | Det ska finnas dokumenterade processer och/eller rutiner för hantering av behörigheter och rättigheter till system. |
| C.3.2 | Varje användare ska ha ett unikt Användar-ID. |
| C.3.3 | Externa användares åtkomst bör vara tidsbegränsad samt föregås av sekretessavtal. |
| C.3.4 | Det ska finnas dokumenterade rutiner för logghantering i objekt. |
| C.3.5 | Höga skyddskrav på konfidentialitet, riktighet eller tillgänglighet innebär också höga krav på spårbarhet. Loggning av användares aktiviteter i sådana system är obligatorisk. |
| C.3.6 | Då regelstyrd behörighetshantering används istället för teknisk behörighetshantering är loggning av användares aktiviteter obligatorisk. |
| C.3.7 | Förändringar i anställningar och roller ska omedelbart rapporteras till personalavdelningen så att reglering av behörigheter kan ske. |
| C.3.8 | Uppföljning ska ske av behörighetshantering och logghantering i objekt. |

## C4. Ändringshantering

Ändringar i system ska ske på ett strukturerat sätt för att säkra systemets säkerhet, funktionalitet och användbarhet och för att minimera antalet fel orsakade av förändringen.

Ändringar kan bero på exempelvis, önskemål från verksamhet/användare, fel eller brister, förändringar i legala krav eller nya versioner från systemleverantörer.

Ändringar i system ska vara samordnade med Change management-processen inom den IT-nära förvaltningen. I Kapitel D som riktar sig till den

IT-nära förvaltningen finns riktlinjer som rör bl.a. systemtest och hantering av testdata (avsnitt D7 – Anskaffning och utveckling av IT-resurser).

Avveckling av system ska ske på ett strukturerat sätt och i samråd med arkivarien så att information hanteras i enlighet med den kommungemensamma riktlinjen för arkivprocessen.

Större förändringar i eller omkring ett system ska föregås av en riskanalys (se avsnitt C6 – Riskanalyser) och godkännas av objektägaren.

| **Riktlinjer för ändringshantering** | |
|---|---|
| C.4.1 | Det ska finnas dokumenterade processer eller rutiner för hantering av ändringar i system. |
| C.4.2 | Vid avveckling av system ska en plan upprättas för hur information ska migreras, raderas eller slutarkiveras (i enlighet med den kommungemensamma riktlinjen för arkivprocessen). |
| C.4.3 | Större ändringar ska föregås av riskanalys och godkännas av objektägaren innan ändring sker. |

## C5. Användarinstruktioner

Objektägare ansvarar för att det finns användarinstruktioner för samtliga användare till ett system. Användare ska utbildas enligt instruktionerna och kontroll ska göras att instruktionerna efterlevs. Användarinstruktionerna ska omfatta följande delar inom informationssäkerhet:

- Regler kring inloggning och lösenordshantering.
- Behörigheter.
- Särskilda instruktioner för hur **konfidentiell** information får hanteras, t.ex. känsliga eller skyddade personuppgifter.
- Information om vad som loggas och konsekvenser av att bryta mot användarinstruktioner, t.ex. att ta del av eller sprida **konfidentiell** information.
- Incidentrapportering – användare ska vara vaksamma på brister och incidenter i systemet och veta hur man ska rapportera dessa (se avsnitt C7 – Incidenthantering).
- Eventuell sekretessförbindelse.

| **Riktlinjer för användarinstruktioner** | |
|---|---|
| C.5.1 | Informationssäkerhetsregler ska finnas med i användarinstruktioner. |
| C.5.2 | Det ska finnas särskilda instruktioner för hantering av konfidentiell information som t.ex. skyddade personuppgifter. |

## C6. Riskanalyser

Risker är tänkbara oönskade händelser som kan inträffa och som kan ha en negativ påverkan på mål. Antingen på mål med själva systemet eller på verksamheters mål. En risk är en kombination av hur sannolikt det är att en händelse inträffar och vilken konsekvens händelsen innebär.

Vid större förändringar, t.ex. större systemuppdateringar, nyutveckling, nya användargrupper eller extern åtkomst, ska en riskanalys genomföras där Vårgårda kommuns grundmetod för riskanalys ska användas. Det kan också vara förändringar utanför själva systemet eller dess kontroll som motiverar en riskanalys, exempelvis ägarbyte av en systemleverantör eller en omorganisation som berör den verksamhet som systemet stödjer. Riskanalysens resultat ska dokumenteras. En riskanalys kan leda till åtgärdsbehov som behöver genomföras omedelbart eller på lite längre sikt och kan då tas med i kommande systemförvaltningsplan.

| **Riktlinjer för riskanalyser** | |
|---|---|
| C.6.1 | Riskanalyser ska genomföras i samband med större förändringar i eller omkring system. |
| C.6.2 | Riskanalysresultat ska dokumenteras. Akuta risker ska tas om hand skyndsamt och återstående åtgärder ska tas med i systemförvaltningsplaner. |

## C7. Incidenthantering

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan, eller skulle kunnat, leda till brister i konfidentialitet, riktighet eller tillgänglighet hos information. Objektägare ansvarar för att incidenter relaterade till system upptäcks, samlas in, hanteras, sammanställs och dokumenteras. Incidenter kan delas in i mindre incidenter och allvarliga incidenter.

Mindre incidenter är t.ex. mindre tekniska fel i system eller att enstaka användare inte följer användarinstruktioner. I systemets användarinstruktioner ska det finnas rutiner för hur användare ska rapportera mindre incidenter (se C5 – Användarinstruktioner). Incidentrapporter ska mottas och lämpliga åtgärder ska vidtas.

Allvarliga incidenter är större störningar i ett system som t.ex. ett längre avbrott (några timmar eller mer), dataintrång eller infektion av skadlig kod. En allvarlig incident kräver en utredning där dokumentation ska göras. Utredningen ska drivas av systemförvaltare i samverkan med relevanta aktörer, inte minst Incident manager och Problem manager på IT-avdelningen.

Systemförvaltare ska i systemförvaltningsplanen ta fram avbrottsplaner att använda vid större avbrott och som ska innehålla ansvarsförhållanden, kontaktpersoner, eskaleringsvägar till interna och externa aktörer. Här ska samverkan ske med den IT-avdelningen.

Flera fall av mindre incidenter av likadan art kan tillsammans utmynna i eller utgöra en allvarlig incident. Ett antal störningar i systemet av samma typ som var för sig betraktas som mindre incidenter kan tillsammans innebära en allvarlig incident. Både mindre och allvarliga incidenter kan vara av akut art och behöva åtgärdas skyndsamt.

Systemförvaltare ska årligen sammanställa samtliga incidenter som är kopplade till systemet och rapportera dessa till Informationssäkerhetsrådet. Kvarstående åtgärdsbehov som inträffade incidenter medfört ska tas om hand i systemförvaltningsplaner.

| **Riktlinjer för incidenthantering** | |
|---|---|
| C.7.1 | Det ska finnas rutiner för hur användare ska rapportera incidenter. |
| C.7.2 | Akuta incidenter ska åtgärdas skyndsamt. |
| C.7.3 | Allvarliga incidenter ska utredas och dokumenteras. |
| C.7.4 | Avbrottsplaner ska upprättas som innehåller ansvarsförhållanden, kontaktpersoner och eskaleringsvägar. |
| C.7.5 | Samtliga incidenter som rör objektet ska dokumenteras, sammanställas och rapporteras till Informationssäkerhetsrådet. Kvarstående åtgärdsbehov ska tas om hand i systemförvaltningsplaner. |

## C.8 Kontinuitetshantering

Krav på kontinuitet av driften av system sker i stora delar genom klassning. **Höga skyddskrav** för tillgänglighet innebär högre krav på säkerhetskopiering och redundans.

Avbrott kan dock ändå alltid ske oavsett vilka förebyggande skyddsåtgärder som finns. Beroendet av funktionalitet i system kan ibland vara så högt att system helt enkelt inte får ligga nere. I dessa fall måste verksamheten ha planer och rutiner för att kunna fullfölja sitt åtagande även vid systemavbrott.

Nyckelpersonsberoende ska undvikas och i den mån det framkommer att organisationen är beroende av nyckelpersonal ska nyckelpersonberoendet åtgärdas t.ex. genom utbildning av ersättare. Nyckelpersonsberoende kan också minskas genom att använda vedertagen standard och standardprodukter.

| **Riktlinjer för kontinuitetshantering** | |
|---|---|
| C.8.1 | Reservplaner och manuella rutiner ska finnas för kritiska objekt med höga skyddskrav gällande tillgänglighet. |
| C.8.2 | Nyckelpersonsberoende ska undvikas och åtgärdas. |

D

# Kapitel D: Informationssäkerhet i IT-miljön

# Inledning

Detta kapitel innehåller riktlinjer rörande säkerhet Vårgårda kommuns IT-miljö. Riktlinjerna vänder sig därför främst till chefer och medarbetare inom Vårgårda kommuns IT-organisation. Riktlinjerna riktar sig också till externa parter som arbetar på uppdrag åt Vårgårda kommun, exempelvis inhyrda konsulter.

Informationssäkerhet i IT-miljön kan även benämnas IT-säkerhet och innefattar säkerhet i olika slag av IT-resurser som system, verktyg och infrastruktur i form av hård- och mjukvara. Termen IT-resurser används genomgående i kapitlet på detta sätt som ett generellt samlingsnamn om ingen specifik hård- eller mjukvara avses.

Kapitlet är strukturerat utifrån nedanstående avsnitt i standarden SS-ISO/IEC 27 002:2014 som till största delar innehåller säkerhet i IT-miljöer:

| Avsnitt | | Kapitel i 27002 |
|---|---|---|
| D1 | Hantering av tillgångar | 8 |
| D2 | Styrning av åtkomst | 9 |
| D3 | Kryptering | 10 |
| D4 | Fysisk och miljörelaterad säkerhet | 11 |
| D5 | Driftsäkerhet | 12 |
| D6 | Kommunikationssäkerhet | 13 |
| D7 | Anskaffning och utveckling av IT-resurser | 14 |
| D8 | Incidenthantering | 16 |
| D9 | Kontinuitetshantering | 17 |
| D10 | Granskning och kontroll (även B7) | 18 |

ISO-Standarden innehåller mer vägledning och information än vad som finns i dessa riktlinjer, och standarden kan därför användas som ett stödjande dokument för att efterleva riktlinjerna.

Inom vissa områden i IT-miljön behöver mer detaljerade instruktioner tas fram som kompletterar eller konkretiserar dessa riktlinjer. Även för detta ändamål kan denna eller andra standarder liksom andra vägledningar, från t.ex. MSB, vara till stöd.

En central del i kommunens informationssäkerhetsarbete är informationsklassning. Information kan ha normala eller **höga skyddskrav** avseende konfidentialitet, riktighet och tillgänglighet i enlighet med Vårgårda kommuns klassningsmodell (se Kapitel B). IT-resurser som hanterar information ska ges ett skydd i enlighet med dessa skyddskrav. Särskilda regler gäller i vissa fall för information som klassats enligt **höga skyddskrav** i en eller flera av aspekterna konfidentialitet, riktighet och tillgänglighet. Detta markeras genomgående med fetstil och rader i tabeller med riktlinjer har dubblerade linjer.

## Roller och ansvar

Ansvar för informationssäkerhet och IT-säkerhet inom IT-avdelningen följer ordinarie verksamhetsansvar. Det innebär att chefer och medarbetare inom respektive ansvarsområde ansvarar för att upprätthålla rätt nivå av

informations- och IT-säkerhet för de processer och de IT-resurser de ansvarar för.

Ytterst ligger ansvaret på IT-chef i egenskap av chef för IT-avdelningen. Därigenom är IT-chef ytterst ansvarig för att säkerheten i informationshantering och IT-miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheters krav, legala krav samt informationssäkerhetspolicyn och dessa riktlinjer för informationssäkerhet.

### IT-säkerhetsansvarig

Den IT-säkerhetsansvarige samordnar arbetet med säkerheten i Vårgårda kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Ansvaret för säkerheten i IT-resurser ligger inte på den IT-säkerhetsansvarige, utan dennes roll är att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av säkerhet i dessa.

För den IT-säkerhetsansvarige innebär detta i huvudsak att:

- utforma och förvalta riktlinjer och instruktioner för IT-säkerhet,
- stödja verksamheter i IT-säkerhetsfrågor,
- följa upp och granska efterlevnaden av riktlinjer och instruktioner för IT-säkerhet,
- stödja och bevaka framtagning och genomförande av handlingsplaner för att åtgärda brister som konstaterats i samband med säkerhetsgranskningar eller riskanalyser,
- bistå vid utredning av misstänkta och inträffade säkerhetsincidenter,
- stödja verksamheter vid extern kravställning rörande IT-säkerhet och uppföljning av externa leverantörers säkerhetsåtaganden,
- leda eller delta i verksamheters riskanalyser rörande IT-relaterade risker,
- verka för höjande av säkerhetsmedvetande inom IT,
- ta fram statusrapporter för kommunens IT-säkerhet, och
- besvara revisionsrapporter.

Den IT-säkerhetsansvarige arbetar nära kommunens informationssäkerhetsansvarige och ingår i Vårgårda kommuns informationssäkerhetsråd. Den IT-säkerhetsansvarige ska också omvärlds-bevaka, nätverka och samverka externt inom området.

### Roller i den IT-nära förvaltningen

Vårgårda kommun har beslutat att tillämpa ett ledningssystem för informationssäkerhet (LIS). Till det tillkommer IT-avdelningens egna styrande dokument med inriktning, riktlinjer och regler. Detta kapitel kompletterar de riktlinjerna med särskilda riktlinjer rörande informationssäkerhet i den IT-nära förvaltningen. Kapitel C riktar sig till den

verksamhetsnära förvaltningen och innehåller informationssäkerhetsrelaterade riktlinjer för denna.

I en verksamhet ska det finnas en utsedd ägare för aktuella system och som då har ansvaret för säkerheten i systemet. Det ska då finnas utsedda ansvariga på IT som kan fungera som motpart till dessa roller så att rätt nivå av säkerhet kan uppnås.

#### Tjänsteansvarig

Tjänsteansvarig ansvarar för att IT-säkerheten i system överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls och att aktuella IT-resurser ges ett skydd som motiveras av klassningen av system. Tjänsteansvariges motsvarighet i den verksamhetsnära förvaltningen är systemägare/systemförvaltare verksamhet.

Tjänsteansvarig ska arbeta för och samverka med informationssäkerhetsansvarige för att Vårgårda kommuns informationssäkerhetspolicy och dessa riktlinjer efterlevs.

#### Processledare-IT

Ansvarar för att IT-processer som anges i kapitel A-C efterlevs. Samverkar och tar fram processer för verksamhetens efterlevnad.

#### Leveransforum

Leveransforum samverkar med systemägare/systemförvaltare verksamhet och i det ansvaret ingår att IT-säkerhetsrelaterade mål och åtgärder i system nås respektive genomförs.

#### IT-Tekniskt ansvarig (specialister)

IT-Tekniskt ansvarig ansvarar för att utföra IT-säkerhetsrelaterade aktiviteter på uppdrag av systemägare/systemförvaltare, ägare av IKT-objekt eller IT-säkerhetsansvarig, eller andra chefer och ansvariga inom IT.

## D1. Hantering av tillgångar

#### Identifiering av IT-resurser och tilldelning av ägare

Samtliga IT-resurser ska vara identifierade och tilldelade en ägare. En förteckning över alla IT-resurser ska upprättas och underhållas.

System som omfattas av verksamheten, exempelvis verksamhetssystem, har naturliga ägare i verksamheterna och stöd av IT-avdelningen i form av tjänsteansvarig. Andra IT-resurser ska ha utpekade ägare.

#### Klassning av IT-resurser

IT-resurser ska klassas i enlighet med Vårgårda kommuns modell för informationsklassning, KLASSA. Verksamhetssystem som klassats av den verksamhetsnära förvaltningen ska ges en nivå av IT-säkerhet som överensstämmer med verksamhetens krav så att rätt säkerhetsnivå upprätthålls. Underliggande IT-resurser i form av infrastruktur, stödsystem

m.m. ska ges minst motsvarande klassning. Ibland kan sådana underliggande IT-resurser ges en högre klassning än de verksamhetssystem som de stödjer, exempelvis om IT-system stödjer ett flertal system som var för sig inte är kritiska.

Om det inte går att göra en koppling mellan IT-resurser och till klassade verksamhetssystem, får man klassa IT-resursen utifrån en bedömning enligt konsekvensbeskrivningarna i klassningsmodellen. Vid osäkra fall är det viktigt att hellre ”överklassa” än ”underklassa”.

Beroende på hur IT-resurser är klassade ska olika säkerhetsåtgärder införas för att uppnå ett tillräckligt bra skydd. Bland annat ska dessa riktlinjer följas som riktar sig mot IT-miljön och som i vissa fall har särskilda krav för IT-resurser som hanterar information med **höga skyddskrav** enligt en eller flera aspekter av konfidentialitet, riktighet och tillgänglighet. Ägare till IT-resurser ansvarar för att säkerhetsnivån är tillräcklig över IT-resursens hela livscykel, såväl vid införande, under drift som under avveckling.

### Användningsinstruktioner

Det ska finnas regler och instruktioner till hur IT-resurser får användas. Dessa ska baseras på IT-resursernas klassning och skyddskrav enligt ovan. Regler och instruktioner ska finnas oavsett om IT-resursen endast används inom IT-avdelningen, av medarbetare inom kommunen eller av externa användare. De som använder eller har tillgång till IT-resurser ska få instruktioner om hur de hanterar dessa resurser, vilka villkor och vilket ansvar som gäller kring den åtkomst de fått sig tilldelad.

Regler och instruktioner kan exempelvis avse användning av:

- Nätverk; t.ex. hur åtkomst till nätverk får ske, hur nätverkstjänster får användas, hur autentisering ska ske och hur utrustning som ansluts till nätverk ska identifieras.
- Operativsystem; t.ex. hur åtkomst och autentisering ska ske.
- Klientdatorer; t.ex. regler för programinstallationer som utförs av användare.

| **D 1 Riktlinjer för hantering av tillgångar** | |
|---|---|
| D.1.1 | Samtliga IT-resurser ska identifieras och tilldelas en ägare med rollerna tjänsteansvarig och systemägare/systemförvaltare verksamhet. |
| D.1.2 | En komplett förteckning över samtliga IT-resurser ska upprättas och underhållas. Rutiner ska finnas för att hålla förteckningen aktuell och den ska skyddas från åtkomst eller förändring av obehörig. |
| D.1.3 | IT-resurser ska klassas baserat på klassningen av den information som hanteras i IT resursen och/eller baserat på klassningen av andra objekt som IT-resursen stödjer eller påverkar. |
| D.1.4 | Skyddsåtgärder i en IT-resurs ska motsvara dess klassning så att rätt nivå av IT-säkerhet upprätthålls under IT-resursens hela livscykel, såväl vid införande, under drift som efter avveckling. |
| D.1.5 | Informationssäkerhetskrav som gäller användandet av IT-resurser ska förmedlas till användare i form av användningsinstruktioner. |

## D2. Styrning av åtkomst

Styrning av åtkomst är grundläggande för att skydda information och IT-resurser. Behörigheter innebär vissa rättigheter att använda informationsobjekt, exempelvis ett system, på ett specificerat sätt. Behörigheter, eller åtkomsträttigheter, definierar vad en användare har rätt att utföra, t.ex. läsa, söka, skriva, radera, skapa eller köra ett program.

Grundprincipen är att behörighetstilldelning ska baseras på användares behov till information eller till de IT-resurser (system, databaser, operativsystem eller nätverk) som dessa behöver för att kunna utföra sina arbetsuppgifter. Om information är strukturerad och klassad är det betydligt enklare att upprätta åtkomstregler och behörighetstilldelningar.

Inom vissa områden kan man behöva ha (teknisk) behörighet till en stor mängd information. Det kan vara svårt att på förhand definiera arbetsuppgifter, eller i akuta situationer måste kanske annan personal än den ordinarie snabbt ha åtkomst till information, som t.ex. inom vård och omsorg. Då får teknisk åtkomstkontroll ersättas av regelstyrd åtkomstkontroll, där regler säger att man inte får ta del av information som inte rör ens arbetsuppgifter. I sådana system är det särskilt viktigt med funktioner för uppföljning, övervakning och loggning.

Det samlade systemet för styrning av åtkomst i en (eller flera) IT-resurs(-er) benämns behörighetskontrollsystem (BKS) och utgörs vanligen av både tekniska system och administrativa rutiner. Ett BKS omfattar tre grundläggande säkerhetsåtgärder som tillsammans ska se till att verksamhetens säkerhetsregler (kontinuerligt) följs:

- Identifiering och autentisering av användares uppgivna identitet.
- Reglering av åtkomsträttigheter; vilken information man kommer åt och vad man kan göra med den, t.ex. läsa, skriva, ändra, radera.
- Loggning av användarens aktiviteter.

### Identifiering och autentisering

Identifiering innebär att aktiviteter och åtkomst till en IT-resurs kan knytas till en individ, därför ska alla användar-ID vara unika och personliga.

Användar-ID och lösenord ger tillsammans en möjlighet till autentisering, dvs. verifiering av en uppgiven identitet. Vid åtkomst till information med **höga skyddskrav** avseende konfidentialitet och/eller riktighet ska stark autentisering användas. Som stark autentisering räknas identifiering av en person och verifiering av personens autenticitet genom en kombination av minst två av följande tre delar:

- Ett lösenord eller någonting annat **som man vet**.
- Ett smartkort eller någonting annat **som man har**.
- Ett fingeravtryck eller någon annan egenskap **som man är**.

Stark autentisering är också krav vid extern åtkomst till Vårgårda kommuns IT-miljö.

Lösenord är alltid **konfidentiella** och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. Det innebär att rutiner ska finnas som säkerställer att lösenordet skyddas t.ex. från administratör eller handläggare oavsett om lösenordet tilldelas, förändras eller återställs.

| **Riktlinjer för identifiering och autentisering** | |
|---|---|
| D.2.1 | Alla användare ska ha en unik användaridentitet. |
| D.2.2 | Namn på användare, som underlag för t.ex. e-postadresser, ska vara enhetliga i kommunen och stämma överens med folkbokföringen. |
| D.2.3 | Vid åtkomst till information med höga skyddskrav avseende konfidentialitet eller riktighet ska stark autentisering användas. |
| D.2.4 | Stark autentisering är krav vid fjärråtkomst till Vårgårda kommuns IT-miljö. |
| D.2.5 | Fjärråtkomst för inloggning med administrativa (priviligierade) konton till IT-resurs med höga skyddskrav avseende konfidentialitet eller riktighet är som regel inte tillåtet. Informationssäkerhetsrådet beslutar om undantag. |
| D.2.6 | Lösenord är alltid konfidentiell information som har höga skyddskrav och ska i alla skeden av sin livscykel skyddas mot åtkomst från alla andra än ägaren själv. För att minska risken för obehörig åtkomst ska följande skyddsfunktioner införas:<br>Tekniska funktioner implementeras där så är möjligt i IT-resursen för att säkerställa att lösenordsregler för medarbetare avseende historik, komplexitet och åldring av lösenord följs.<br>Lösenord ska aldrig skickas/transporteras i klartext över nätverk. I de fall detta inte är möjligt ska tillfälliga lösenord i kombination med tvingande lösenordsbyte användas. Tillfälliga lösenord ska enbart vara giltiga för en (1) inloggning.<br>Om felaktigt lösenord används mer än åtta gånger ska aktuellt användar-ID utestängas en viss tid ur systemet och händelsen loggas. |
| D.2.7 | För att minska risken för obehörig åtkomst ska samtliga klienter (datorer samt mobila enheter) förses med låsskärm så att skärm automatiskt låses efter en definierad tids inaktivitet och enbart kan aktiveras igen genom en förnyad autentisering. |

### Reglering av åtkomsträttigheter

Åtkomst till IT-resurser ska baseras på dess klassning, exempelvis ställs större krav på metoder för autentisering vid åtkomst till information med **höga skyddskrav** (se ovan).

För verksamhetssystem är det systemägare i verksamheten som beslutar vilka som ska få tillgång till systemet och vilka behörigheter dessa ska ha, samt hur systemet är klassat. Tjänsteansvarig IT ansvarar för att upprätta ett BKS som motsvarar dessa krav.

Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser. Detta inkluderar att underhålla och förvalta behörigheter, exempelvis hantering av beställning, ändring och borttagning av behörigheter och rättigheter. Förändringar i användares roller måste återspeglas i behörighetshanteringen, t.ex. att användare får andra arbetsuppgifter eller avslutar sin anställning.

Det ska finnas en process kopplad till personalavdelningen där man säkerställer att reglering av åtkomst sker vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning.

Innan någon tilldelas åtkomst till IT-resurs som innehåller uppgifter **konfidentiell** information, ska alltid prövning av den enskilde ske och en tystnads- och sekretessförbindelse upprättas och den enskilde ska utbildas i vad förbindelsen innebär och vilket ansvar som följer.

För externa användare gäller att tilldelning av åtkomst, utöver de regler som gäller all åtkomst-tilldelning även ska vara tidsbegränsad för endast den tiden som behövs för att utföra uppgiften samt föregås av sekretessavtal.

För administrativa åtkomsträttigheter gäller att de ska vara restriktiva och ge endast de rättigheter som behövs för att utföra sitt uppdrag i den administrativa roll man har. Om funktion för privilegiehöjning finns ska sådan användas, t.ex. genom att använda ”sudo” i Linux/Unix eller att man efter inloggning utför vissa aktiviteter med ett konto med förhöjda rättigheter i Windows genom funktionen ”Kör som annan användare”. Vidare ska man där så är möjligt säkerställa att automatisk utloggning sker efter en definierad tids aktivitet vilken bör vara kortare än för normala användare.

Regelbunden uppföljning och revision av samtliga åtkomsträttigheter ska ske kontinuerligt. För priviligierade användare med särskilda åtkomsträttigheter (administratörer) ska revision ske med kortare intervall. Särskild uppmärksamhet kan behöva ägnas då medarbetare med priviligierade åtkomsträttigheter slutar eller byter tjänst. Processer och rutiner för behörighetshantering ska följas upp och dokumenteras.

| Riktlinjer för reglering av åtkomsträttigheter | |
|---|---|
| D.2.8 | Det ska finnas beslutade och dokumenterade regler och rutiner för behörighetshantering, dvs. BKS, i IT-resurser. |
| D.2.9 | IT-resurser ska ha åtkomsträttigheter som motsvarar hur de är klassade. |
| D.2.10 | Användaridentiteter och vilka individer dessa tillhör ska registreras i en gemensam förteckning och rutin ska finnas för att hålla denna förteckning uppdaterad. För att garantera spårbarhet ska rutinen även innehålla kontroll så att inte tidigare identiteter återanvänds. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter som fanns och vilka individer dessa tillhörde vid varje given tidpunkt. |
| D.2.11 | Åtkomst av IT-resurser ska vara registrerade i en förteckning med den åtkomst som beslutats och rutin ska finnas att hålla denna förteckning uppdaterad. Historikfunktion ska finnas så att förteckningen kan visa vilka identiteter och individer som hade åtkomst till en IT-resurs vid en given tidpunkt. |
| D.2.12 | Åtkomst som inte längre behövs eller behov av ny åtkomst ska regleras snarast, för IT-resurser inom en arbetsdag efter att behov upphör eller uppstår. Det ska finnas rutiner kopplade till personalavdelningen för att säkerställa att sådan reglering av åtkomst kan ske vid anställning, vid förändring av roll eller arbetsuppgifter samt vid upphörande av anställning. |
| D.2.13 | Administrativa rättigheter ska endast ges där så är uttryckligen nödvändigt och rättigheterna ska då vara tidsbegränsade. För tilldelning av administrativa rättigheter för användare på klienter gäller att sådan rätt i första hand ska ges tillfälligt för att t.ex. omfatta en installation av |

| | |
|---|---|
| | programvara och i andra hand ges för en viss tid med ett specifikt slutdatum. Tjänsteansvarig IT beslutar om tilldelning av priviligierad åtkomsträtt. Granskning (stickprov) av administrativa rättigheter ska ske en gång per månad. |
| D.2.14 | Gruppidentiteter är inte tillåtna. Eventuella undantag ska godkännas av Systemägare verksamhet och informationssäkerhetsansvarig i förening. Gruppidentiteter ska då enbart beviljas under följande förutsättningar:<br>Behov av gruppidentitet är tydligt beskrivet och alternativen utredda så att det framgår varför gruppidentiteten är nödvändig.<br>Gruppidentiteten ska ha en registrerad ägare.<br>Gruppidentiteten ska vara tidsbegränsade med tydligt slutdatum.<br>En avvecklingsplan ska finnas för att ersätta gruppidentiteten med individuella identiteter.<br>Ägaren av gruppidentiteten ska föra en förteckning alla som använder identiteten. Historikfunktion ska finnas så att förteckningen kan visa vilka användare som fanns vid en given tidpunkt.<br>Autentiseringsinformation ska uppdateras om någon användare lämnar gruppidentiteten. Om en användare t.ex. lämnar en gruppidentitet med ett delat lösenord så ska lösenordet ändras och ett nytt lösenord distribueras till kvarvarande användare av gruppidentiteten.<br>Ägaren av gruppidentiteten tar fullt ansvar för eventuellt missbruk av gruppidentiteten. |
| D.2.15 | För externa användare gäller att tilldelning av åtkomst, utöver övriga regler för åtkomsttilldelning även ska: Tidsbegränsas att endast omfatta tiden som behövs för att utföra uppgiften. Föregås av sekretessavtal. |
| D.2.16 | Prövning av den enskilde ska ske och en tystnads- och sekretessförbindelse upprättas innan åtkomst tilldelas till IT-resurs som innehåller information med höga skyddskrav avseende konfidentialitet. |

### Säkerhetsloggning

För att erhålla spårbarhet och möjliggöra incidentutredningar och att i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser från kommunens regelverk ska kommunens IT-resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informations-säkerhetshändelser. Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet.

I de fall logginformation går att knyta till en enskild person är de att betrakta som personuppgifter och omfattas då av krav i Dataskyddsförordningen. Detta innebär bland annat att sådana loggar med personuppgifter ska skyddas från obehöriga. Det innebär också att om loggning används för att tekniskt övervaka ett system av säkerhetsskäl får loggen inte senare användas för andra syften. Om kontroller utförs för andra syften än det ursprungliga är lagkravet att personen ska informeras och ge sitt samtycke.

| Riktlinjer för säkerhetsloggning | |
|---|---|
| D.2.17 | Vid åtkomst till IT-resurs och information med höga skyddskrav avseende konfidentialitet eller riktighet krävs loggning av åtkomst för att erhålla spårbarhet. |
| D.2.18 | Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst, logginformation innehållande loggning av åtkomst har alltid höga skyddskrav avseende konfidentialitet eller riktighet. |
| D.2.19 | Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser, ska skapas, bevaras en bestämd tid och granskas regelbundet. För loggar som innehåller systemadministratörers aktiviteter gäller att de ska granskas av loggadministratör som inte är samma person som systemadministratören. |

## D3. Kryptering

Kryptering kan användas för flera ändamål, såsom att genom kryptering förhindra obehörig åtkomst till information, eller genom kryptografiska signaturer garantera informationens riktighet eller äkthet.

IT-avdelningen ska vid behov tillhandahålla godkända krypteringslösningar och instruktioner hur dessa ska användas. Behov av kryptering ska baseras på informationsklassning. Vanligen finns behov av kryptering då det föreligger **höga skyddskrav** på konfidentalitet och/eller riktighet.

Krypteringslösningar ska bygga på etablerade standarder som NIST 140-2 eller ISO/IEC 18033 och ska tas fram av tjänsteansvarig IT i samråd med verksamhetsansvarig och IT-säkerhetsansvarig. Införande av krypteringslösningar ska godkännas av informationssäkerhetsansvarig efter prövning i informationssäkerhetsrådet.

Ibland kan krypteringslösningar medföra nya risker relaterade till nyckelhantering. Dessa risker behöver hanteras bl.a. genom revokering (certifikat ogiltigförklaras), validering och återställning av nycklar:

- Revokering av nycklar gör det möjligt att avsluta åtkomst till IT-resurser.
- Validering av nycklars giltighet och autenticitet möjliggör att användare av en IT-resurs kan avgöra om en nyckel är giltig och att innehavaren kan kontrolleras.
- Återställning av nycklar är en funktion för att göra det möjligt att återställa information även om nyckel förloras. Detta kan t.ex. åstadkommas genom användandet av en särskild återställningsnyckel eller genom att nycklar säkerhetskopieras. Dock kan sådana lösningar innebära andra säkerhetsrisker eftersom nycklarna finns på fler ställen, och det ställer stora krav på åtkomstkontroll, administrativa rutiner och loggning så att åtkomst till nycklar kan spåras.

| Riktlinjer för kryptering | |
|---|---|
| D.3.1 | Krypteringslösningar ska baseras på etablerade standarder och införande ska godkännas av informationssäkerhetsansvarig efter prövning av informationssäkerhetsrådet. |
| D.3.2 | Nyckelhantering ska säkerställas för att tillgodose de krav som finns för IT-resurs avseende:<br>Revokering av nycklar.<br>Validering av nycklars giltighet och autenticitet.<br>Återställning av nycklar. |
| D.3.3 | Krypteringsnycklar är konfidentiell information och ska skyddas därefter. |

## D4. Fysisk och miljörelaterad säkerhet

Fysisk och miljörelaterad säkerhet avser att förhindra otillåten fysisk åtkomst till, skador på och störningar i IT-resurser.

Generellt gäller att informationsklassning ska användas som ett stöd för att utforma det fysiska skyddet som alltid måste utgå från vilken information som hanteras samt hur skyddsvärda IT-resurserna är.

### Säkra utrymmen för IT resurser

Säkra utrymmen med särskilda säkerhetskrav är exempelvis rum som används för servrar, switchar och annan kommunikationsutrustning, kontorsutrymmen där känslig information bearbetas samt arkiv. För IT-funktioner är det främst datorhallar, serverrum samt korskopplingsutrymmen som är aktuella.

Tillträden till säkra utrymmen ska vara restriktiva och endast ges till de personer som behöver tillträde för att utföra sitt uppdrag i den roll de har. Det ska finnas dokumenterade beslut om vem som ges tillträde att arbeta i säkra utrymmen.

Roller med ansvar för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas. Personer med arbetsuppgifter i säkra utrymmen ska ha god kännedom om de regler som gäller för arbetet i dessa lokaler.

Säkra utrymmen ska utformas så att utrustning inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp.

Godkänt brandskydd och brandlarm ska finnas. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilation och andra genomföringar mellan brandceller ska förses med brandspjäll.

Säkra utrymmen som innehåller IT-resurser med **höga skyddskrav** ska bevakas och fysisk närvaro ska loggas (t.ex. tillträdes- eller videoövervakningsloggar).

### Godsmottagning och lastning

Utrymme för godsmottagning och lastning ska avgränsas och organiseras så att de begränsar onödigt tillträde till känsliga områden och säkra utrymmen. Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören.

### Underhåll, reparation och avveckling

Underhåll av utrustning ska ske i enlighet med leverantörens anvisningar.

Reparation av utrustning och IT-resurser kräver ofta åtgärder från extern personal och auktoriserade reparatörer med utbildning på den utrustning som ska hanteras. Sådan personal har oftast varken behörighet till den information som hanteras i IT-resursen eller tillträde till sådana säkra utrymmen där IT-resurser finns placerade och detta kräver därför särskild uppmärksamhet.

Om underhåll och reparation ska utföras av utomstående på IT-resurs med **höga skyddskrav** avseende konfidentialitet ska vederbörande alltid underteckna sekretessavtal. Det kan ibland vara nödvändigt att vidta särskilda åtgärder, t.ex. att känslig information flyttas, raderas eller krypteras innan någon utomstående hanterar utrustningen. Detsamma gäller avveckling av IT-resurser där avveckling eller återanvändning bör ske på ett sådant sätt att känslig information inte riskerar att komma i orätta händer. Datamedia där information inte har krypterats kan t.ex. behöva skrivas över eller destrueras på ett säkert sätt innan den sänds till skrotning eller återanvändning.

### Skydd av utrustning

Utrustning ska placeras och skyddas för att skyddas mot stöld och miljörelaterade hot som värme, kyla, fuktighet, vätska samt partiklar i luft. Användning ska ske i enlighet med de instruktioner som framtagits av utrustningens ägare. Riskerna för åverkan och stöld är högre i vissa av kommunens egna lokaler, t.ex. där många externa personer frekvent vistas och i publika lokaler.

Speciellt utsatt är också mobil utrustning där risken för förlust, stöld och skada är högre. Användning ska ske i enlighet med de instruktioner som gäller vid distansarbete och mobil utrustning där användare t.ex. ska säkerställa att utrustning antingen övervakas eller låses in för att minska risken för stöld.

### Elförsörjning

Säker elförsörjning (t.ex. avbrottsfri kraft genom UPS och reservkraft) ska finnas så att IT-resurser skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjnings-system.

| Riktlinjer för fysik och miljörelaterad säkerhet | |
|---|---|
| D.4.1 | Tillträdet till säkra utrymmen ska vara begränsat och regleras minst med hjälp av låssystem med separat nyckelsystem. Nyckel-, kort- och kodinnehav ska vara förtecknade. |
| D.4.2 | Rutiner för att arbeta i säkra utrymmen ska utformas och tillämpas. Roller med ansvar för ett säkert utrymme har också ansvar att ta fram en instruktion för hur arbete i respektive lokal får bedrivas. |
| D.4.3 | Beslut om vem som ges tillträde att arbeta i säkra utrymmen ska vara dokumenterat. |
| D.4.4 | Personal som beviljats tillfälligt tillträde till säkra utrymmen ska övervakas under hela besöket. |
| D.4.5 | Åtkomstpunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna ska styras och om möjligt isoleras från säkra utrymmen med IT-resurser för att undvika säkerhetsrisker. |
| D.4.6 | Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören. |
| D.4.7 | Godkänt brandskydd och brandlarm ska installeras. Släckutrustning ska väljas så att inte onödig skada uppstår vid släckning av brand. Ventilations och andra genomföringar mellan brandceller ska förses med brandspjäll. |
| D.4.8 | Utrymmet ska utformas så att utrustningen inte utsätts för vätskeläckage, korrosiva brand- och släckgaser, damm etc. VA-dragningar i eller i direkt närhet av driftmiljö ska undvikas och risker för vatteninträngning hanteras. Om golvbrunn finns ska åtgärder vidtas för att undvika att vatten kan tränga upp. |
| D.4.9 | Utrymmen som innehåller informationsobjekt med höga skyddskrav ska uppfylla Skyddsklass 3 enligt SSF 200 Inbrottsskydd. |
| D.4.10 | IT-resurser ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem. |
| D.4.11 | Kablage för ström och telekommunikation för data eller stödjande informationstjänster ska skyddas från avlyssning, störningar och skada. |
| D.4.12 | Åtgärder ska vidtas för att temperaturen hålls inom de gränsvärden som specificerats för aktuell utrustning, även vid störningar i elförsörjningen i de fall utrustning försetts med avbrottsfri kraft. |
| D.4.13 | Datamedia som innehåller för verksamheten kritisk information och systeminformation ska förvaras i för datamedia brandklassat datamedieskåp. |
| D.4.14 | Underhåll och reparation ska utföras på sådant sätt att information eller IT-resurs inte riskerar att röjas eller skadas. Om utomstående ska utföra underhåll på IT-resurs med höga skyddskrav ska sekretessavtal tecknas. Vid känslig information döljas, flyttas eller raderas från utrustningen. Underhåll och reparation ska följas upp i loggböcker. |
| D.4.15 | Avveckling eller skrotning av IT-resurser och datamedia ska, efter att information som ska bevaras ha förts över till arkivet, ske genom att information skrivs över, raderas eller förstörs. |
| D.4.16 | Avveckling eller skrotning av datamedia med höga skyddskrav på konfidentialitet sker genom att information skrivs över i multipla operationer, alternativt att mediet där informationen lagrats förstörs på ett fullständigt och oåterkalleligt sätt. Observera att krypterad datamedia inte är känslig om nyckel för dekryptering ges ett fortsatt skydd, eller att nyckel destruerats. |
| D.4.17 | IT-utrustning ska inte avlägsnas utanför kommunens lokaler utan tillstånd. |

## D5. Driftsäkerhet

### Driftsrutiner

Dokumenterade driftsrutiner ska finnas och göras tillgängliga för alla användare som behöver dem. Driftsrutiner ska finnas för väsentliga processer och objekt, såsom:

- installation och konfiguration av system,
- uppstarts- och nedtagningsrutin,
- säkerhetskopiering (se nedan),
- underhåll av utrustning,
- supportkontakter vid oväntade funktionella eller tekniska problem,
- hantering av media och
- datahall (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

Driftsrutiner ska vara formella och beslutade dokument.

Förändringar i IT-resurser ska styras enligt fastställd Change Management-process. Denna process ska säkerställa att alla ändringar som införs på tjänster, moduler och komponenter i IT-miljön är riskbedömda, planerade, kommunicerade, testade och godkända.

Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

| **Riktlinjer för driftsrutiner** | |
|---|---|
| D.5.1 | Det ska finnas formella, beslutade och dokumenterade driftsrutiner för väsentliga processer och objekt. Dessa ska göras tillgängliga för alla användare som behöver dem. |
| D.5.2 | Ändringar i IT-resurser ska följa fastställd process som säkerställer att ändringarna är riskbedömda, planerade, kommunicerade, testade och godkända (ITIL Change Management). |
| D.5.3 | Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön. |

### Skydd mot skadlig kod

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka skadlig kod och för att återställa IT-miljön efter angrepp. Förutom tekniskt skydd är det även viktigt att alla som använder IT-resurser vet hur de kan minska risken att drabbas av skadlig kod samt vad de ska göra om de misstänker angrepp av skadlig kod.

Kommunens IT-resurser ska skyddas från skadlig kod genom att antivirusprogramvara installeras på klienter och servrar. Skyddet ska regelbundet uppdateras. Programvara ska i förebyggande syfte skanna efter skadlig kod i:

- datorer i kommunens nätverk,
- filer som tas emot via nätverk eller någon form av media och i

- webbsidor.

IT-resurser med **höga skyddskrav** ska regelbundet granskas avseende skadlig kod.

Om angrepp av skadlig kod inträffat ska det finnas en fastställd rutin för återställning av IT-resurser (se avsnitt D9 – Incidenthantering).

Säkerhetsuppdateringar är en viktig komponent för att hålla system och applikationer fria från säkerhetsbrister som kan exploateras av skadlig kod.

Det ska finnas rutiner för att regelbundet samla in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se).

| **Riktlinjer för skadlig kod** | |
|---|---|
| D.5.4 | Det ska finnas metoder och programvara för skydd mot skadlig kod som förebygger, upptäcker skadlig kod och som återställer i kommunens IT-miljö efter angrepp. |
| D.5.5 | IT-resurser som stöder objekt med höga skyddskrav ska regelbundet granskas med avseende på skadlig kod. |
| D.5.6 | System och applikationer ska regelbundet uppdateras för att hållas fria från säkerhetsbrister som kan exploateras av skadlig kod. Säkerhetspatchar ska regelmässigt och skyndsamt installeras på alla IT-resurser enligt tillverkarnas rekommendationer och enligt fastställd rutin. |
| D.5.7 | Det ska finnas en fastställd rutin för återställning av datorer om kommunen skulle drabbas av skadlig kod eller virusutbrott. |
| D.5.8 | Det ska regelbundet samlas in information om skadlig kod, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod (t.ex. cert.se). |

### Säkerhetskopiering

Säkerhetskopiering av information, program och speglingar av system är en viktig del av driftsäkerheten. Detta ger möjlighet att återställa en IT-resurs till ett fungerande tillstånd efter uppkomsten av ett fel, och att åtgärda både riktighet och tillgänglighet hos information.

Säkerhetskopieringen syftar till att väsentlig information ska kunna rekonstrueras med hjälp av säkerhetskopior och återlagringsrutiner. Dock är det inte alltid möjligt att återställa all information. Sådan information som tillförts systemet efter senaste säkerhetskopiering går normalt inte att återställa.

Det finns en viktig skillnad mellan säkerhetskopiering och spegling (redundans). Den sistnämnda ger enbart ett skydd för tillgänglighet och inte riktighet, eftersom informationen är identisk vid spegling vilket innebär att eventuell felaktig information då återfinns på båda ställen. Säkerhetskopiering och spegling är tillsammans nödvändiga skyddsåtgärder för IT-resurser med krav på både riktighet och tillgänglighet.

Vilka skyddsåtgärder som vidtas för specifika system ska styras på av hur de är klassade i aspekterna tillgänglighet och riktighet. Stöd för detta kan vara att använda de två måtten RPO och RTO. Hur stor informationsförlust som kan accepteras kan definieras för varje IT-resurs genom att fastställa RPO

(Recovery Point Objective). Den längsta acceptabla tiden för att återställa IT-resursen efter ett avbrott kan fastställas med målsättning för återställningstid RTO (Recovery Time Objective).

Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet för att skydda från fysiska incidenter och katastrofer som t.ex. brand och översvämning. Ofta används lösningar där man skiljer på långtids- och korttidslagring där enbart långtidslagringen är skild från originalmaterialet. Då bör korttidslagring skyddas genom ett säkert utrymme avsett för datamedia, annars riskerar man att vid en brand förlora all information som tillförts systemet sedan kopiering till långtidslagring skedde, vilket i vissa fall kan vara lång tid (se avsnitt D4 – Fysisk och miljörelaterad säkerhet).

Säkerhetskopior ska testas regelbundet för att säkerställa att återlagring fungerar som avsett.

| **Riktlinjer för säkerhetskopiering** | |
|---|---|
| D.5.9 | För IT-resurser med höga skyddskrav avseende tillgänglighet ska redundans finnas i delkomponenter, system, lagring och nätverk samt säkerställd infrastruktur för IT-drift, t.ex. UPS elförsörjning, reservkraft, redundant kyla m.m.<br>Tillgänglighet ska övervakas med automatiska larm om viktiga kvalitetsmått inte uppfylls. Gränsvärden för larm ska sättas så att uppfyllande av målsättning för återställningstid säkerställs. Automatiska larm ska regelbundet testas. |
| D.5.10 | Baserat på objekts klassning av riktighet och tillgänglighet ska krav definieras för säkerhetskopiering av information. Dessa krav ska minst reglera vilken information som ska omfattas av säkerhetskopiering, hur lång tid säkerhetskopior ska sparas samt vilka kontroller som ska genomföras av att säkerhetskopiorna fungerar.<br><br>Vidare ska maximal informationsförlust och målsättning för återställningstid definieras för varje IT-resurs och tillsammans med övriga krav ligga till grund för vald backuplösning.<br><br>Målsättning för återställning av data, RPO (Recovery Point Objective), den maximalt acceptabla mängden av dataförlust som tillåts vid en återställning av en IT-tjänst efter ett avbrott ska fastställas.<br>Målsättning för återställningstid, RTO (Recovery Time Objective), den längsta acceptabla tiden för att återställa IT resursen efter ett avbrott ska fastställas. |
| D.5.11 | Det ska finnas en process för återlagring från säkerhetskopia som är testad och dokumenterad för respektive IT-resurs. |
| D.5.12 | Backup av IT resurser med höga skyddskrav avseende tillgänglighet (höga RTO krav) bör lagras på snabbt backupmedia såsom t.ex. SAN-diskar. Övervakning av backupfunktion ska konfigureras med automatlarm vid problem. |
| D.5.13 | Säkerhetskopiering av information med höga skyddskrav avseende konfidentialitet ska ske till krypterad backupmedia eller ges motsvarande skydd. Säkra återställningsrutiner ska användas med kontroller att återställning av konfidentiell information ges rätt skydd efter återställning, t.ex. bör dekryptering under återställning undvikas. |
| D.5.14 | Säkerhetskopior ska lagras geografiskt åtskilt från originalmaterialet. Om lösning används där man skiljer på långtids- och korttidslagring är det tillräckligt att långtidslagringen är skild från originalmaterialet under förutsättning att korttidlagrade säkerhetskopior förvaras i ett säkert utrymme avsett för datamedia. |

### Lagring och övervakning

Övervakning och loggning gör det möjligt att upptäcka händelser i IT-resurser. Genom loggning kan man i efterhand analysera vad som hänt och på så sätt möjliggöra korrigerande eller förebyggande åtgärder. Händelseloggar som registrerar användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser ska skapas, bevaras och granskas regelbundet.

Loggning av händelser utgör grunden för automatiserade övervakningssystem som är kapabla att skapa konsoliderade rapporter och varningar avseende säkerhet i system och tillämpningar.

Händelseloggar kan innehålla bl.a.

- användarkonto,
- systemaktiviteter,
- datum, tider och uppgifter om viktiga händelser, t.ex. inloggning och utloggning,
- enhetens identitet eller plats, om möjligt, och systemidentifierare,
- register över lyckade och misslyckade åtkomstförsök till system,
- poster av lyckade och misslyckade åtkomstförsök till data och andra resurser,
- förändringar i systemkonfiguration,
- användning av privilegierad åtkomst,
- användning av systemverktyg och tillämpningar,
- åtkomst till filer och typ av åtkomst,
- nätverksadresser och protokoll,
- alarm från systemet för åtkomstkontroll,
- aktivering och inaktivering av säkerhetsverktyg, som anti-virussystem och intrångsdetekteringssystem, och
- register över transaktioner som utförs av användare i tillämpningar.

Krav på loggar och övervakningssystem kan variera beroende på IT-resursens art och användningsområde. Det är IT-resursens klassning och objektägarens krav som utgör grunden för behovet.

Genom användning av loggverktyg samt att alla loggkällor använder gemensam och korrekt tid kan händelser i olika IT-resurser korreleras vilket ger en bättre och mera heltäckande bild av händelser jämfört med om logg övervakas i varje system för sig.

Loggar kan innehålla känsliga data och personinformation. Lämpliga säkerhetsåtgärder för ska därför vidtas.

| Riktlinjer för loggning och övervakning | |
|---|---|
| D.5.15 | Loggning ska normalt ske i IT-resurser avseende fel, systemhändelser. Loggar ska sparas en viss tid samt regelbundet analyseras och övervakas. Typ och omfattning av loggar och övervakningssystem ska baseras på IT-resursers klassning och objektägares krav. |
| D.5.16 | För att säkerställa all typ av loggning av händelser ska systemklockorna i alla relevanta IT-resurser synkroniseras mot en betrodd referenskälla för korrekt tid. |
| D.5.17 | Loggningsverktyg och logginformation har höga skyddskrav och ska skyddas mot manipulation och obehörig åtkomst. |

### Hantering av tekniska sårbarheter

Tekniska sårbarheter i IT-resurser kan innebära exponering för skadlig kod, dataintrång eller andra sårbarheter. Det ska finnas rutiner så att information om tekniska sårbarheter erhållas i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

Okontrollerad installation av program kan medföra sårbarheter och incidenter, som exempelvis obehörig åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter. Regler för programinstallationer som utförs av användare ska upprättas och införas som definierar vilka typer av program en användare kan installera och på vilket sätt.

| Riktlinjer för hantering av tekniska sårbarheter | |
|---|---|
| D.5.20 | Det ska finnas rutiner för att få information om, upptäcka, analysera och åtgärda tekniska sårbarheter i IT-resurser. Uppdateringar och säkerhetspatchningar ska göras regelbundet på IT-resurser. |
| D.5.21 | I de fall säkerhetspatchning inte är praktiskt möjlig, t.ex. för ”embedded” system eller SCADA-system ska information om tekniska sårbarheter i sådana IT-resurser inhämtas och analyseras och lämpliga åtgärder vidtas för att hantera den tillhörande risken. |
| D.5.22 | Säkerhetsgranskning av IT-resurser som exponeras mot Internet ska ske regelbundet och minst en gång per år för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. bestå av skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. |
| D.5.23 | Det ska finnas regler för programinstallationer som utförs av användare som definierar vilka typer av program en användare kan installera och på vilket sätt. |

## D6. Kommunikationssäkerhet

Kommunikationssäkerhet är skydd i IT-resurser och nätverk som används för data-kommunikation i syfte att skydda den information som kommuniceras.

### Nätverkssäkerhet

Nätverk måste hanteras och styras för att skydda information i anslutna system och tillämpningar. Det ska finnas rutiner för hantering av nätverk och förvaltning ska ske av ansvariga som utpekas av ägare till nätverk.

Skyddsåtgärder ska införas för att nå säkerhet för information i nätverk och anslutna tjänster utifrån klassningen av anslutna objekt, dvs. krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. Skydd för nätverkssäkerhet kan exempelvis vara:

- Autentisering av system.
- Kryptering.
- Regler för säkerhet och nätverksanslutning.
- Begränsning av systemanslutningar.
- Brandväggar och intrångsdetekteringssystem.
- Loggning och övervakning av nätverk.
- Separation av nätverk (segmentering).

Segmentering betyder att dela upp nätverket i olika segment för att t.ex. tillåta enbart ekonomiadministratörer tillgång till nätverket med ekonomisystem. Segmentering av nätverk ska användas som en del av den totala säkerhetslösningen för att skydda känslig information och övriga resurser.

En grundläggande segmentering av nätverket ligger i att skilja interna nät från Internet, samt att utvecklings-, test- och produktionsmiljöer ska vara skilda från varandra. Ytterligare segmentering ska göras då det är motiverat av säkerhetsskäl. Brandväggar och utrustning för segmentering av nätverk behöver revideras regelbundet för att hållas uppdaterade med rätt regler för kommunikation mellan olika IT-resurser över de olika nätsegmenten.

| **Riktlinjer för nätverkssäkerhet** | |
|---|---|
| D.6.1 | Krav på skydd vad gäller nätverkstjänster ska identifieras, dokumenteras och tillämpas samt inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster. |
| D.6.2 | Trådlös datakommunikation innehållande information med normala eller höga skyddskrav avseende konfidentialitet är endast tillåtet från godkända klienter. Teknik för att kryptera och säkra kommunikationen (minst WPA2 PSK) ska alltid användas oavsett skyddskrav. |
| D.6.3 | En grundläggande segmentering av nätverket ska göras för att skilja interna nät från Internet, samt att skilja utvecklings-, test- och produktionsmiljöer från varandra. Grupper av informationstjänster, användare och informationssystem kan ytterligare segmenteras i separata nätverks efter skyddsbehov. |
| D.6.4 | Brandväggar ska konfigureras i enlighet med dokumenterad brandväggspolicy. Av brandväggspolicyn ska framgå vilka nätverkstjänster som ska tillåtas, vilka händelser och aktiviteter som ska loggas och följas upp. Brandväggar och brandväggspolicyer ska revideras periodiskt. |
| D.6.5 | Kommunikationstjänster mellan Vårgårda kommun och externa nätverk ska dokumenteras och godkännas av Objektägare IT innan inkoppling får ske. |

Informationsöverföring

Information som hanteras genom elektronisk meddelandehantering ska ges lämpligt skydd. Om e-post innehållande information med **höga skyddskrav** avseende konfidentialitet ska sändas till extern part ska lösning med kryptering och signering användas.

Avtal som reglerar säker överföring av verksamhetsinformation mellan Vårgårda kommun och extern part ska upprättas. Användandet av osäkra klartextprotokoll såsom t.ex. FTP och HTTP ska undvikas och ersättas av säkra alternativ om information med normala eller **höga skyddskrav** avseende konfidentialitet ska överföras.

| **Riktlinjer för informationsöverföring** | |
|---|---|
| D.6.6 | Kommunikation med höga skyddskrav avseende konfidentialitet och riktighet ska alltid krypteras och kommunicerande parter ska identifieras på ett säkert sätt med digitala signaturer eller motsvarande. |
| D.6.7 | Utgående massutskick av e-post ska begränsas för att förhindra att kapad mailbox används till att skicka ut stora mängder spam. |
| D.6.8 | Överföringslösningar för verksamhetsinformation mellan Vårgårda kommun och externa parter ska regleras genom avtal där minst följande regleras:<br>Motparten informeras om informationens klassning och garanterar att information med normala eller höga skyddskrav avseende konfidentialitet ges rätt nivå av skydd och inte förs vidare till annan part.<br>Kommunikationslösning ska definieras med de nätverkskomponenter som ingår i säkerhetslösningen samt den konfiguration och de inställningar som krävs för att upprätthålla rätt nivå av skydd.<br>Vid kommunikation med annan part med normala eller höga skyddskrav avseende konfidentialitet ska överföringen skyddas med kryptering.<br>Trafik i uppsatta förbindelser ska loggas av båda parter. |
| D.6.9 | Kommunikation med e-post till andra organisationer skyddas i samtliga e-postsystem genom att konfigurera och aktivera standardiserade säkerhetsfunktioner såsom SPF, DKIM och krypterad SMTP över TLS. |
| D.6.10 | E-post med höga skyddskrav avseende konfidentialitet till extern mottagare ska krypteras och signeras. E-post med höga skyddskrav enbart avseende riktighet ska kryptografiskt signeras men behöver inte krypteras. |

## D7. Anskaffning och utveckling av IT-resurser

Korrekt informationssäkerhet för IT-resurser ska säkerställas över hela livscykeln och börjar vid anskaffning eller utveckling.

### Säkerhetskrav på IT-resurser

Krav som rör informationssäkerhet ska redan från början inkluderas i kraven för nya IT-resurser likväl som i krav för förbättringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardsystem).

Informationssäkerhetskraven ska spegla den klassning som tilldelats IT-resursen och som baseras på t.ex. författningar och interna regelverk, riskanalyser eller analys av incidenter.

Utveckling, anskaffning eller förändring av system som omfattas av verksamhetsnära förvaltning ska involvera parterna i

förvaltningsorganisationen. Objektägare IT ansvarar för att rätt tekniska krav formuleras som överensstämmer med verksamhetens krav så att system ges skydd som korrelerar till klassningen.

Utveckling, anskaffning eller förändring av underliggande IT-resurser i form av infrastruktur, stödsystem m.m. ska ha minst motsvarande krav som de system som de stöder. Ibland kan kraven vara ännu högre än för de system de stödjer, exempelvis om en IT-resurs stödjer ett stort antal system som var för sig inte är kritiska.

Informationssäkerhetskrav ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas.

| **Riktlinjer för säkerhetskrav på IT-resurser** | |
|---|---|
| D.7.1 | Informationssäkerhet ska inkluderas i kraven för nya IT-resurser i förändringar av befintliga. Det gäller oavsett om IT-resursen upphandlas externt, utvecklas internt eller en kombination av båda (t.ex. anpassning av ett inköpt standardsystem).<br><br>Informationssäkerhetskraven ska baseras på den klassning som tilldelats IT-resursen och ska dokumenteras och granskas av alla berörda parter innan utvecklingen, anskaffningen eller förändringen påbörjas. |

### Säkerhetskrav vid upphandling av IT-stöd

Vid upphandling av IT-stöd gäller ovanstående riktlinjer för säkerhetskrav på IT-resurser. Det är än viktigare vid extern upphandling att vara tydlig när det gäller kravställning av informationssäkerhet. Externa leverantörer använder kanske annan terminologi och har annan förståelse för informationssäkerhet än vad som föreligger internt i kommunen. Exempelvis är man kanske inte familjär med klassning av information och objekt, och även om man är det kanske man tillämpar andra nivåer och tolkar de olika nivåerna på annat sätt.

Avtal med IT-leverantör ska reglera ansvar för implementation och upprätthållande av säkerhetsfunktioner och ansvar för testning och verifiering av dessa. Dessutom ska avtalet reglera ansvar för sådana brister som eventuellt upptäcks under drift.

Om upphandlade system även ska driftas hos en leverantör tillkommer krav som kan innefatta:

- Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar).
- Leverantörens kontinuitetshantering.
- Rätt till tredjepartsrevision.
- Sekretessavtal.
- Personuppgiftsbiträdesavtal.

- Rätt till incidentrapporter från leverantören.

I kravspecifikationer ska alltid tydliga krav på säkerhet formuleras som sedan används vid utvärdering av anbud. Upphandling av IT-stöd ska alltid göras i samverkan med ansvarig för upphandling och uppföljning.

Vårgårda kommun kommer att ta fram kravkataloger som baseras på hur objekt är klassade (se avsnitt B6 – Leverantörsrelationer).

| **Riktlinjer för säkerhetskrav vid upphandling av IT-stöd** | |
|---|---|
| D.7.2 | Tydliga informationssäkerhetskrav ska ställas vid upphandling av IT-stöd och ska sedan användas vid utvärdering av anbud. Kraven ska baseras på den klassning som tilldelats IT-resursen. |
| D.7.3 | IT-leverantörer ska alltid delge hur de bedriver säkerhetsarbete i såväl den operativa verksamheten som avseende säker systemutveckling. |
| D.7.4 | Avtal med IT-leverantör ska innefatta stöd och support i händelse av fel och incidenter. |
| D.7.5 | Avtal med IT-leverantör ska reglera hur kontroll av avtalets uppfyllande ska ske, t.ex. genom tredjepartsrevision eller granskning genomförd av Vårgårda Kommun. |
| D.7.6 | Upphandling av system som ska driftas hos extern leverantör medför ytterligare krav, exempelvis:<br>Fördjupade krav på leverantörens interna IT-miljö och informationssäkerhet (t.ex. certifieringar).<br>Leverantörens kontinuitetshantering.<br>Rätt till tredjepartsrevision.<br>Sekretessavtal.<br>Personuppgiftsbiträdesavtal.<br>Rätt till incidentrapporter från leverantören. |
| D.7.7 | Upphandling av IT-stöd ska göras i samverkan med ansvarig för upphandling. |
| D.7.8 | För att säkerställa tillgänglighet till källkod samt underhåll och utveckling i händelse av oväntade förändringar hos IT-leverantör eller dess underleverantörer ska så kallad källkodsdeposition användas, där minst ett exemplar av källkoden lämnas i förvar hos tredje part. |
| D.7.9 | Avtal med IT-leverantör ska innefatta:<br>Att leverantören innan leverans till Vårgårda kommun genomför säkerhetstestning av system och ingående komponenter.<br>Att testet genomförs av tredje part.<br>Att leverantören ska åtgärda eventuella säkerhetsbrister som identifierats i samband med acceptanstest och/eller leveranskontroll. |
| D.7.10 | Om IT-leverantör använder underleverantör för hela eller del av leveransen ska ett avtal tecknas dem emellan som reglerar såväl affärsmässighet som säkerhet. Avtalet ska kunna delges. Följande punkter ska då minst beaktas avseende säkerhet:<br>Hur applicerbara krav i avtal med IT-leverantör säkerställs även mot dess underleverantör.<br>Hur rättsliga krav uppfylls, exempelvis rörande lagstiftning om sekretess och personuppgifter.<br>Vilka åtgärder som vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt.<br>Vilka åtgärder som vidtas för att säkerställa kvalitet i leverans från underleverantör. |

### Säkerhet vid systemutveckling

Processer och rutiner ska finnas på plats för att säkerställa att informationssäkerhet designas och införs under utvecklingscykeln av IT-resurser. Säkerhet måste vara en integrerad del i utvecklingsprocessen, från början till slut. Regler för säker utveckling av program och system ska upprättas och tillämpas vid systemutveckling.

Systemförändringar inom utvecklingscykeln ska styras genom användning av Change management-processen.

För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel. En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverad i systemutveckling och integration. Det innebär även att alla utvecklare måste ha en grundkompetens i programvarusäkerhet och att utvecklingsprocesser innehåller komponenter av utbildning och omvärldsbevakning.

Outsourcad systemutveckling ska övervakas och styras och säkerhetsfunktionalitet ska säkerställas vid utveckling. Dessa modeller kan användas i kravställningen runt utvecklingsprocesser beroende på vilken metod utvecklingsleverantören använder. Om ingen etablerad modell används av leverantören krävs en betydligt mer ingående analys för att säkerställa en säker utvecklingsprocess.

| **Riktlinjer för säkerhet vid systemutveckling** | |
|---|---|
| D.7.11 | Processer, rutiner och regler ska finnas som reglerar att informationssäkerhet finns med under hela utvecklingscykeln av IT-resurser. |
| D.7.12 | Systemförändringar inom utvecklingscykeln ska styras genom användning av Change management-processen. |
| D.7.13 | För systemutvecklings- och integrationsåtgärder ska utvecklingsmiljöer upprättas och skyddas över IT-resursens hela livscykel. |
| D.7.14 | Systemutvecklare ska ha kompetens i programvarusäkerhet. |
| D.7.15 | Vid outsourcad systemutveckling ska krav ställas att man tillämpar en etablerad modell för säker systemutveckling. |

### Säkerhetskrav vid test

Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling. Vid test kan man dra nytta av automatiserade verktyg, t.ex. verktyg för kodgranskning eller för skanning av sårbarheter. Testning bör utföras i en realistisk testmiljö för att säkerställa att systemet inte kommer att införa sårbarheter i organisationens miljö och att testerna är tillförlitliga.

Testdata bör skyddas och kontrolleras. System- och acceptanstest kräver normalt avsevärda mängder testdata som är så snarlika produktionsdata som möjligt. Att använda produktions-databaser för test bör undvikas och personuppgifter måste i så fall först anonymiseras.

Test-, utvecklings- och driftmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön. Utvecklare ska inte tillåtas att testa icke fastställda och godkända programversioner eller förändringar i driftmiljö.

Driftsättning ska ske enligt Change management-processen.

| **Riktlinjer för säkerhetskrav vid test** | |
|---|---|
| D.7.16 | Säkerhetsfunktionalitet ska testas vid utveckling och testning ska göras gentemot de ställda säkerhetskraven och i enlighet med riktlinjer för säker utveckling. |
| D.7.17 | Produktionsdata ska inte användas i test utan all testdata ska väljas ut noggrant, skyddas och styras. Om produktionsdata ändå behöver används gäller följande:<br>Testdata ska alltid anonymiseras från personuppgifter.<br>Rutiner för styrning av åtkomst som tillämpas för produktionssystem ska också gälla vid test av sådana system.<br>Behörighet ska godkännas av objektägare IT varje gång produktionsdata kopieras till ett testsystem.<br>Produktionsdata ska omgående raderas från testsystem efter avslutad test.<br>Kopiering av produktionsdata ska loggas för att erhålla spårbarhet. |
| D.7.18 | Test- eller utvecklingsversioner får ej placeras i produktionsmiljö utan utvecklings-, test och driftmiljöer ska separeras för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön. |
| D.7.19 | Driftsättning ska ske enligt Change management-processen. |

## D8. Incidenthantering

Med informationssäkerhetsincident avses en händelse som har eller skulle kunnat ha försämrat konfidentialitet, riktighet eller tillgänglighet hos information.

Alla medarbetare i Vårgårda kommun är skyldiga att rapportera incidenter (se Kapitel A). Detta innefattar självklart även medarbetare på IT-avdelningen samt externa aktörer som exempelvis konsulter. Även svagheter i skydd (brister) ska rapporteras, exempelvis larm som inte fungerar, öppna dörrar till våra lokaler eller öppna fönster efter kontorstid osv. IT- och informationsrelaterade incidenter och brister ska rapporteras till IT-support.

Processer och rutiner ska finnas på plats för att säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation i samband med incidenterna.

För IT används ITIL-processen ”Incident Management”. Denna process innefattar fler typer av incidenter än vad som kan definieras som informationssäkerhetsincident enligt ovan, men incidenthanteringsprocessen måste självklart omfatta och hantera informationssäkerhetsincidenter. Dessa kan vara av olika typer, exempelvis:

- Obehöriga har fått tillträde till kommunens lokaler.
- Obehöriga har kommit åt information.

- Dokument, till exempel publika rapporter, har ändrats felaktigt eller utan behörighet.
- Infektion av virus eller annan skadlig kod.
- Information som borde ha funnits arkiverad har försvunnit.
- IT-resurser missbrukas av medarbetare eller externa personer.

Viktiga aktiviteter i incidenthanteringsprocessen är:

- Mottagning av information om incidenten.
- Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats.
- Analys av orsaker till incidenten så att korrektiva och preventiva åtgärder kan vidtas.
- Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten.

Incident manager leder hanteringen av incidenter i samverkan med berörda ägare av objekt. Vid incidenter relaterade till verksamhetsnära objekt ska incident managern samverka med relevanta roller i förvaltningsorganisationen.

Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen.

Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar.

Kunskaper baserade på analyser av hanterade incidenter ska användas för att minska sannolikheten eller konsekvenser av framtida, liknande, incidenter. Kort sagt bör man lära av sådant som har inträffat så att man kan vidta åtgärder för att förhindra återupprepning. Vissa åtgärder kan behöva vidtas skyndsamt och i samband med att en incident inträffar.

Större incidenter ska sammanställas i incidentrapporter som respektive objektägare ansvarar för att ta fram i samverkan med incident manager. Mindre incidenter ska registreras och sammanställas och kan ligga till grund för kvantifiering och statistik.

Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.

| Riktlinjer för incidenthantering | |
|---|---|
| D.8.1 | Det ska finnas en incidenthanteringsprocess på IT som omfattar informationssäkerhetsincidenter. Processen ska innefatta:<br>Mottagning av information om incidenten.<br>Styrning av eventuella behov av omedelbara åtgärder. Dessa kan vara av temporär art tills en mer hållbar lösning kan komma på plats.<br>Analys av orsaker till incidenten så att korrektiva och preventiva åtgärder kan vidtas.<br>Återkoppling och kommunikation med dem som är påverkade av eller involverade i återhämtning efter incidenten liksom till den som rapporterat incidenten. |
| D.8.2 | Större incidenter ska sammanställas i incidentrapporter som respektive objektägare ansvarar för att ta fram i samverkan med incident manager. |
| D.8.3 | Erfarenheter från inträffade incidenter, t.ex. genom incidentrapporter och statistik, ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar. |
| D.8.4 | Medarbetare är skyldiga att rapportera informationssäkerhetsincidenter såväl som informations- och IT-relaterade brister i system eller tjänster. |
| D.8.5 | Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas och insamling av bevis m.m. ska inte göras utan samråd med polisen. Medarbetare och deltagare i verksamheten som har upptäckt en incident eller svaghet där brott misstänks föreligga, ska inte själva försöka bevisa detta då det kan försvåra utredningar. |

### Krisorganisation och krisplan

En krisplan ska finnas som ska aktiveras vid händelse av allvarliga incidenter eller kriser (s.k. major incidents) i IT-miljön. Krisplanen ska ha en ansvarig förvaltare och innehålla bl.a. krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris.

| Riktlinjer för krisorganisation och krisplan | |
|---|---|
| D.8.6 | Det ska finnas en krisorganisation på IT-avdelningen för allvarliga incidenter och kriser som tydligt beskriver roller och ansvar. |
| D.8.7 | Det ska finnas en krisplan på IT som ska aktiveras vid händelse av en allvarlig incident eller kris. Krisplanen ska bl.a. innehålla krisorganisation, kontaktpersoner och operativa steg att vidta under en allvarlig störning eller kris. |
| D.8.8 | Krisplanen ska testas och övas minst en gång per år. Identifierade brister och svagheter ska åtgärdas i syfte att ständigt förbättra krisplanen för IT. |

## D9. Kontinuitetshantering

Kontinuitetshantering innebär att man i en organisation systematiskt arbetar med att och skapa en god återhämtningsförmåga för kritiska verksamhetsprocesser och minimera konsekvenserna av störningar, avbrott och katastrofer. Arbetet innefattar att identifiera kritiska verksamhets-processer och dessas beroenden av stöd och resurser som t.ex. personal, lokaler och verktyg.

IT-resurser är ofta viktiga stöd för kritiska verksamhetsprocesser som ibland kan vara helt beroende av att det finns tillgängligt och fungerar som avsett. Kontinuitetshantering för IT är därför en viktig del i informationssäkerhetsarbetet för att minimera negativa konsekvenser vid allvarliga IT-relaterade incidenter eller avbrott. Syftet är att efter ett större avbrott så snabbt som möjligt återgå till normalläge och att konsekvenserna

för verksamheten ska vara så små som möjligt, både under och efter avbrottet.

Detta innebär att det för objekt med **höga skyddskrav** avseende tillgänglighet måste finnas en beredskap för hur man hanterar avbrott – s.k. avbrottsplaner. Objektägare IT ansvarar för att avbrottsplaner finns på plats och att de motsvarar de krav som finns för objekt. Avbrottsplaner ska vara relaterade till incidenthanteringen och den övergripande krisplan som ska finnas på IT-avdelningen (se avsnitt D8). En viktig säkerhetsåtgärd för att skapa och bibehålla hög tillgänglighet är säkerhetskopiering (se avsnitt D5).

Målsättningen är att kontinuitetshantering ska utvecklas i hela Vårgårda kommun och på sikt ingå i ett ledningssystem för informationssäkerhet (se avsnitt A4).

| **Riktlinjer för kontinuitetshantering** | |
|---|---|
| D.9.1 | Det ska finnas avbrottsplaner för samtliga kritiska IT-resurser med höga skyddskrav avseende tillgänglighet. |
| D.9.2 | Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet och identifierade brister samt svagheter åtgärdas med syfte att ständigt förbättra kontinuiteten för IT. |
| D.9.3 | Avbrottsplaner ska finnas tillgängliga för de medarbetare som ingår i aktiviteterna, men samtidigt utgör planerna information med högt skyddsvärde och förvaras skyddat så att de inte blir åtkomliga för obehöriga. |

## D10. Granskning och kontroll

Granskning av IT-säkerhet för IT-resurser ska ske regelbundet för att kontrollera att inga uppenbara sårbarheter exponeras och att tillräcklig säkerhetsnivå upprätthålls. Sådan granskning kan t.ex. vara skanning av sårbarheter med automatiserade verktyg eller så kallade penetrationstester. Särskilt viktigt är det att genomföra kontroll och granskning av kritiska delar av IT-miljön som direkt eller indirekt stöder system med höga skyddsvärden, samt införande av nya IT-lösningar.

Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. Rapportering av större sårbarheter och brister ska ske till informationssäkerhets-rådet.

Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Revision eller mätning av Vårgårda kommuns informationssäkerhet i stort kan även omfatta IT-miljön.

| **Riktlinjer för granskning och kontroll** | |
|---|---|
| D.10.1 | Kritiska delar i IT-miljön som stödjer objekt med höga skyddsvärden ska regelbundet övervakas och granskas för att sårbarheter och brister ska upptäckas. |
| D.10.2 | Nya IT-lösningar ska vid minsta osäkerhet gällande säkerhetsförhållanden utsättas för tekniska granskningar av extern part (t.ex. penetrationstester). |

| | |
|---|---|
| D.10.3 | Sårbarheter och brister som upptäcks vid granskningar ska tas upp för åtgärdande i genomförandeplaner, t.ex. förvaltningsplaner. Akuta sårbarheter och brister ska åtgärdas omedelbart. |
| D.10.4 | Rapportering av större sårbarheter och brister ska ske till informationssäkerhetsrådet. |
| D.10.5 | Revision av hela eller stora delar av IT-miljön ska göras minst vartannat år. Innan granskning eller revision kan ske ska följande beaktas:<br>Behov på åtkomst till system och data inför granskning eller revision ska avtalas med objektägare.<br>Omfattningen av tekniska aktiviteter för granskning eller revision ska beskrivas för- och godkännas av IT-resursens ägare.<br>Aktiviteter vid granskning eller revision begränsas om möjligt till skrivskyddad åtkomst av program och data.<br>Granskning som kan påverka tillgänglighet bör utföras under servicefönster eller vid sådan tidpunkt då påverkan på verksamheten är så liten som möjligt.<br>All åtkomst vid granskning eller revision ska övervakas och loggas |

## Resurser och länkar

Informationssäkerhet för medarbetare

DinSäkerhet.se

En sida om risker och säkerhet för privatpersoner. DinSäkerhet drivs av MSB – Myndigheten för samhällsskydd och beredskap.

DinSäkerhet.se - Informationssäkerhet

Direktlänk till avsnittet om informationssäkerhet där det finns information om hur man skyddar sin information och IT-miljö i hemmet och privat.

DISA – Datorstödd informationssäkerhetsutbildning för användare

Den utbildning som tillhandahålls gratis av MSB och som anknyter till Kapitel B i dessa riktlinjer.

Krisinformation.se

Krisinformation.se är en webbplats som drivs av MSB och förmedlar information från myndigheter och andra ansvariga till allmänheten före, under och efter en stor händelse eller kris.

Stöldskyddsföreningen

Säkerhetsinformation m.m. för både privatpersoner och företag. Viss information finns om informationssäkerhet, bl.a. surfa säkert och ID-stölder.

**Övriga kapitel**

MSB

Myndigheten för samhällsskydd och beredskap, MSB, är en statlig myndighet med uppgift att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. MSB har i uppgift att samordna arbetet med samhällets informationssäkerhet.

MSB – Informationssäkerhet

Direktlänk till sidorna på MSB om informationssäkerhet. Här finns en hel del publikationer i form av vägledningar, handböcker m.m.

Informationssäkerhet.se

På informationssäkerhet.se finns stöd för hur man arbetar med systematisk informations-säkerhet i organisationer. Informationssäkerhet drivs av MSB i samverkan med PTS, Polisen, Säpo, FRA, FMV och Försvarsmakten.

CERT-SE

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verk-samheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

CERT-SE agerar operativt då IT-incidenter inträffar genom informationsspridning och samordning, samverkar med myndigheter med särskilda uppgifter inom informationssäkerhets-området och är Sveriges kontaktpunkt gentemot andra länder.

Dataföreningen

Dataföreningen har nätverk och utbildningar inom informationssäkerhet och ordnar seminarier m.m.

SIG Security

SIG Security är en svensk intresseförening för de som arbetar professionellt inom området IT- och informationssäkerhet. SIG Security ordnar seminarier och pubkvällar m.m., främst i Stockholm.

SIS - informationssäkerhet

SIS – Swedish Standards Institute – är Sveriges standardiseringsorgan och publicerar de svenska standarderna inom informationssäkerhetsområdet, främst den s.k. 27000-serien.

SIS ordnar seminarier och konferenser och ger utbildningar i Informationssäkerhetsakademin.