# Vägledning för fysisk informationssäkerhet i it-utrymmen

# Vägledning för fysisk informationssäkerhet i it-utrymmen

Vägledning för fysisk informationssäkerhet i it-utrymmen

Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet
Faktaunderlag: Mikael Gustafsson.

Layout: Advant Produktionsbyrå AB
Tryckeri: DanagårdLiTHO

Publ.nr: MSB629 - december 2013
ISBN: 978-91-7383-401-8

# Innehåll

# Förord

Informationshantering är ett centralt stöd för alla typer av verksamheter. Det blir därmed allt viktigare att kunna skydda informationen för att samhället ska fungera på ett robust sätt och för att tillgången till information ska kunna säkerställas både på kort och på lång sikt.

En viktig faktor för att kunna skydda informationen är det fysiska skydd som omger olika typer av it-utrymmen. Att planera, utveckla och förvalta it-utrymmen innebär ett stort ekonomiskt åttagande där det inte alltid är lätt att avgöra vilka åtgärder som är lämpliga och rimliga för att ge informationen ett tillräckligt bra skydd. Myndigheten för samhällsskydd och beredskap (MSB) har ansvar för att samordna arbetet med samhällets informationssäkerhet. Riksarkivets främsta uppgift är att säkerställa samhällets behov av en långsiktig informationsförsörjning som garanterar innehåll, sammanhang och äkthet.

I båda dessa uppdrag är en väsentlig del att ge stöd till organisationer för att skydda information. För att underlätta för både myndigheter och andra organisationer att utforma it-utrymmen på ett säkert sätt har MSB och Riksarkivet tillsammans tagit fram denna vägledning.

Stockholm 20 december

**Helena Lindberg**
*Generaldirektör*
Myndigheten för
samhällsskydd och beredskap

**Björn Jordell**
*Riksarkivarie*
Riksarkivet

# Inledning

# 1. Inledning

## 1.1 Syfte

Syftet med denna vägledning är att ge olika typer av organisationer, både offentliga och privata, ett stöd för att den fysiska informationssäkerheten i förvaring och användning av it-utrustningar ska motsvara de krav på skydd som respektive organisation har. Vägledningen syftar också till att ge myndigheter stöd för att kunna efterleva de krav på skydd av allmänna handlingar som ställs i arkivlagen och efterföljande föreskrifter från Riksarkivet som gäller skydd av digital information.

## 1.2 Målgrupp

Målgruppen är it-ansvariga, informationssäkerhetsansvariga, it-säkerhetsansvariga, fastighetsansvariga, arkivansvariga, it-arkivarier, projektörer och upphandlare som på något sätt involveras i planering, nyproduktion eller förändring av utrymmen såsom datorhallar, serverrum, kommunikationsutrymmen eller liknande typer av lokaler.

## 1.3 Bakgrund

Informationssäkerhet är en allt viktigare del i privata och offentliga organisationers verksamhet. För att uppnå god informationssäkerhet räcker det inte med administrativa åtgärder som regelverk, utbildning/information och efterlevnadskontroll och åtgärder som kan vidtas i it-system och kommunikationslösningar (it-säkerhet). Utrustning för informationshantering måste också skyddas från olika risker, det vill säga fysiskt skydd eller fysisk it-säkerhet.

Området fysiskt skydd inom informationssäkerhet omfattar ett antal delområden som denna vägledning kommer att behandla. För att underlätta den fortsatta läsningen kommer här att ges en allmän bakgrund samt några viktiga avgränsningar.

### 1.3.1 Informationssäkerhet och fysiskt skydd

Informationssäkerhet handlar om styrning av skydd till lämplig nivå för varje informationsmängd. Detta gäller även styrning av utformningen av fysiskt skydd. Ett systematiskt informationssäkerhetsarbete bygger på att säkerhetsåtgärder vidtas utifrån de risker verksamhetens informationshantering är utsatt för. Det innebär att en organisations fysiska skydd, bland annat datorhallar, ska motsvara de krav som kommer fram i riskanalys och informationsklassningar. Det är alltså verksamhetens behov som ska styra skyddet. It-utrymmen är en stor ekonomisk investering och det är därför mycket viktigt att säkerhetsåtgärderna är anpassade efter behoven, det vill säga är vare sig under- eller överdimensionerade. Är de underdimensionerade innebär det oacceptabla risker för organisationen, är de överdimensionerade innebär det en oacceptabel kostnad.

**Ansvar och roller**

En annan viktig del i det systematiska informationssäkerhetsarbetet är tydligt ansvar och roller. Ledningen har alltid det övergripande ansvaret men det opera-

tiva ansvaret för it-utrymmena måste delegeras till tydliga roller i organisationen. Det är ofta lämpligt att skilja på rollerna som ansvarig för it-utrymmena respektive ansvarig för it. Den som är ansvarig för it kan då bli en beställare till den som är ansvarig för fastighetsfrågor exempelvis. På så sätt uppnås att respektive roll har den bästa kompetensen samt en tydlig rollfördelning.

Trots att organisationer ofta har investerat betydande belopp för att förbättra säkerheten i sina it-utrymmen är det relativt vanligt att man saknar en adekvat organisation som upprätthåller den säkerhetsnivå man har investerat i.

En särskilt viktig aktivitet ur informationssäkerhetssynpunkt är då it-utrymmen planeras/projekteras eller byggs om. I dessa skeden är det nödvändigt att genomföra riskanalyser och informationsklassningar samt integrera säkerhetsarbetet i hela projektet.

För en organisation som arbetar systematiskt med informationssäkerhet är det viktigt att definiera olika skyddsnivåer som motsvarar resultatet i informationsklassningen. Att ha definierade skyddsnivåer underlättar väsentligt för upphandling och outsourcing. I bilaga 1 finns ett exempel på hur skyddsnivåer kan utformas inom fysiskt skydd.

**Referenser**
Inom alla informationssäkerhetsområden finns i dagsläget en stor mängd av referenser. Vanliga benämningar som PUL, ISO/IEC-27000-serien, ISO/IEC-20000, PCI-DSS, NERC-CIP, ISF, SOX, HIPAA är alla exempel på lagar, standarder, branschnormer och andra typer av referenser[1]. Inom det fysiska informationssäkerhetsområdet existerar det motsvarande typer av referenser som behandlar, reglerar och styr implementation av olika typer av skydd.

Intentionen i denna vägledning är inte att göra en strikt redovisning av referensers innehåll, hur olika referenser förhåller sig till varandra eller andra liknande redogörelser. Referenser kommer dock att redovisas i vägledningen där detta bedöms som viktigt, framförallt för att öka förståelsen och då framförallt referenser som är vanliga eller tillämpas i Sverige. I undantagsfall kommer andra branschspecifika, nationella och internationella referenser att nämnas i vägledningen.

1. Krav på skydd av allmänna handlingar ställs på myndigheter genom arkivlagen och Riksarkivets föreskrifter. Riksarkivet har utfärdat föreskrifter om elektroniska handlingar, RA-FS 2009:1, och föreskrifter för arkivlokaler, RA-FS 2013:4.

### FÖRVARING OCH SKYDD AV ALLMÄNNA HANDLINGAR

Allmänna handlingar är handlingar (oavsett medium) som har inkommit till eller upprättats hos en myndighet och som förvaras hos myndigheten. De allmänna handlingarna bildar myndigheternas arkiv. Utgångspunkten är att allmänna handlingar ska bevaras och att gallring endast får ske under vissa förutsättningar. Krav på skydd av allmänna handlingar ställs på myndigheter genom arkivlagen och Riksarkivets föreskrifter. Riksarkivet, vars föreskriftsrätt omfattar statliga myndigheter, har utfärdat föreskrifter om elektroniska handlingar, RA-FS 2009:1, och föreskrifter för arkivlokaler, RA-FS 2013:4.

Riksarkivets föreskrifter om arkivlokaler består dels av generella bestämmelser som ska tillämpas på information oavsett medium (analogt och digitalt), dels av bestämmelser för mediespecifik information. I denna vägledning har vi försökt att endast lyfta fram de bestämmelser som gäller oavsett medium. Vårt ställningstagande är att om det förvaras allmänna handlingar i it-utrymmen (exempelvis datorhall eller datorrum) ska tillämpliga bestämmelser för arkivlokaler gälla även för dessa utrymmen.

Handlingar som tillhör myndighetens arkiv ska förvaras i en lokal som ger skydd mot vatten och skadlig fukt; brand, brandgas och skadlig upphettning; skadlig klimat- och miljöpåverkan samt skadegörelse, tillgrepp och obehörig åtkomst. Vid val av lokalens placering ska myndigheten undersöka om den omgivande miljön är lämplig med hänsyn till dessa skyddskrav. Riskbedömningar måste därför göras av miljön både inom och utanför byggnaden.

Vid planeringen av ett it-utrymme där allmänna handlingar ska förvaras, eller vid planeringen av ändringar i ett sådant utrymme, ska myndigheten inhämta Riksarkivets yttrande. Myndigheten ska bl.a. komma in med dokumentation som beskriver arkivlokalens utformning och tänkta placering. Riksarkivet har även rätt att inspektera myndighetsarkivet, inkl. den fysiska förvaringen av de allmänna handlingarna. Riksarkivet ska därför alltid ges möjlighet att inspektera förvaringen oavsett arkivets fysiska placering.

### 1.3.2 Olika typer av utrymmen

I denna vägledning föreslås ett antal krav och rekommendationer för utformning av olika typer av it-utrymmen. Där det finns avvikelser för statliga myndigheters fysiska skydd av allmänna handlingar framgår det i vissa fall i form av en fotnot och hänvisning till relevant föreskrift. Observera att de krav som ställs för skydd av allmänna handlingar på myndigheter är desamma oavsett om myndigheten har upphandlat en förvaringslösning hos en annan myndighet eller enskild leverantör eller förvarar informationen i egna lokaler. Vid outsourcing ska myndigheten genom en skriftlig överenskommelse säkerställa att den som förvarar arkivet tillämpar Riksarkivets föreskrifter.

Alla typer och varianter av lokaler ryms inte i en text som denna vägledning utan de kommer att generaliseras till tre typer. Observera att det förekommer ett stort antal benämningar som här sammanfattas i tre huvudtyper:

- **Datorhall**
  Med en datorhall avses en lokal som förvarar en större mängd it-utrustningar. Lokalen är initialt avsedd och projekterad för it-drift.
- **Datorrum**
  Med datorrum avses en lokal som förvarar en mindre mängd it-utrustningar. Lokalen kan vara anpassad för it-drift, men är inte uttalat avsedd eller projekterad för det ändamålet.
- **Kommunikationsrum/Korskopplingsrum (KK-rum)**
  Ett KK-rum är en lokal där kommunikationsutrustningar såsom routers, switchar och hubbar kopplas samman. Lokalen kan vara anpassad för it-drift. I ett KK-rum förvaras ingen utrustning som innehåller datamedia (hårddiskar, databand, disketter eller liknande).

Dessa tre generaliserade typer av lokaler anges vidare med en gemensam benämning – **it-utrymmen**. It-utrymmen avser samtliga typer av lokaler som är avsedda för it-drift och förvarar it-utrustning[2].

## 1.4 Avgränsningar

### 1.4.1 Säkerhetsskydd

På vissa verksamheter ställs krav på säkerhetsskydd med stöd av säkerhetsskyddslagen. Denna vägledning omfattar dock inte åtgärder som ska vidtas med stöd av säkerhetsskyddslagstiftningen. För stöd i sådana frågor hänvisas till Rikspolisstyrelsen och Försvarsmakten som utfärdar föreskrifter och utövar tillsyn på området inom respektive ansvarsområde.

### 1.4.2 Redundans

Redundans eller dubblering är ett fenomen som har blivit allt vanligare det senaste decenniet, framförallt hos verksamheter med större mängder utrustning och/eller kritiska it-system. Den tekniska utvecklingen, framförallt inom virtualisering och lagringsteknik, har avsevärt förenklat processen att dubblera funktioner och öka toleransen mot störningar.

Att skapa redundanta lösningar är en viktig men komplex fråga som det inte finns utrymme att gå närmare in på i denna vägledning[3].

### 1.4.3 Upphandling

Många organisationer väljer att köpa plats i it-utrymmen istället för att bygga och underhålla egna lösningar. På detta sätt slipper man många arbetsmoment och man kan anpassa behovet av kvadratmeteryta för stunden. Ökar behovet av plats så köper man mer yta, minskar antalet utrustningar och it-system köper man mindre yta.

Denna vägledning kommer inte att närmare gå in på upphandlingssituationen utan hänvisar till den vägledning för upphandling av it-relaterade tjänster som MSB tidigare har tagit fram. De principer som där beskrivs kan även tillämpas i stort då det gäller upphandling och outsourcing av it-utrymmen[4].

2. Enligt Riksarkivets definition är arkivlokal en lokal som är anpassad för förvaring av arkiv. Om det förvaras allmänna handlingar i it-utrymmen (exempelvis datorhall eller datorrum) ska lokalen följaktligen definieras som arkivlokal och omfattas av de bestämmelser som gäller för arkivlokaler (RA-FS 2013:4).
3. Riksarkivet har bl.a. krav på att elektroniska handlingar ska bevaras i flera exemplar med identiskt informationsinnehåll (RA-FS 2009:1, 4 kap. 17 §).
4. Vägledning – informationssäkerhet i upphandling, MSB555, www.msb.se

### 1.4.4 Bärbar utrustning och utrustning utanför organisationens lokaler

Idag hanteras allt mer information via olika typer av bärbar utrustning samt i utrustning utanför organisationens egna lokaler. Även i dessa situationer finns ofta behov av fysiskt skydd. Dessa aspekter kommer dock inte att behandlas i denna vägledning utan vi hänvisar där till MSB:s vägledning för säkrare hantering av mobila enheter[5].

### 1.4.5 Datamedia och säkerhetskopiering

Elektronisk information som behandlas, lagras eller transporteras i eller utanför ett it-utrymme utnyttjar alltid någon typ av elektronisk utrustning som innehåller media (datamedia). Olika datamedia har olika egenskaper vilket påverkar valet av lämpliga skyddsåtgärder. I denna vägledning kommer dock ingen mer utförlig diskussion att föras kring detta på grund av skriftens begränsade omfattning, och inte heller kring säkerhetskopiering. Dock finns i bilaga 3 en rekommendation kring förvaring av säkerhetskopior.

### 1.4.6 Personskydd och arbetsmiljö

Vid byggnation eller ombyggnation av ett it-utrymme finns det skäl att ta hänsyn även till arbetsmiljö och personskydd. Dessa frågor kommer inte att behandlas i denna vägledning som är helt inriktad på informationssäkerhet.

5. Vägledning för säkrare hantering av mobila enheter, MSB405, www.msb.se

# Säkerhetsområden för it-utrymmen

# 2. Säkerhetsområden för it-utrymmen

Innehållet i kapitlets avsnitt kommer att stegvis behandla säkerhetsaspekter hos it-utrymmen. Inledningsvis kommer uppbyggnaden, själva grundkonstruktionen, att diskuteras och därefter följer specifika områden som inbrottsskydd, brandskydd, tillträdesskydd och säkerhet i infrastruktur som el, kyla och vätska. Området inredning i it-utrymmen samt teknisk övervakning behandlas också i separata delkapitel.

Det är dock viktigt att redan från början understryka att säkerheten i it-utrymmena inte endast beror på tekniska lösningar utan i hög grad även på de organisatoriska förutsättningar som ledningen i organisationen ger. Den centrala frågan är i detta sammanhang att ansvar och roller måste vara mycket tydliga. I denna vägledning kommer inte den organisatoriska säkerheten att diskuteras ytterligare men i bilaga 2 finns en checklista som stöd för att ta fram lämpliga rutiner för driften av it-utrymmen.

## 2.1 Placering

Var en verksamhet väljer att placera sina it-utrymmen kan betyda mycket för en ökad säkerhet. Om en incident sker utanför ett it-utrymme kan placering vara en avgörande faktor för att minimera riskerna för att it-utrustning och datamedia kommer till skada. Placeringen av it-utrymmen bör därför vara väl genomtänkt för att undvika yttre hot samt minska konsekvenserna om hoten realiseras.

Tyvärr är det vanligt att it-utrymmen är bristfälligt placerade. I äldre fastigheter är en riskfylld placering vanligare, men även medvetet riskfyllda placeringar av it-utrymmen i nybyggnationer förekommer.

> Översvämningen i Göteborgsregionen år 2006 medförde att vatten från närliggande vattendrag trängde in i flera verksamheters it-utrymmen med omfattande driftstörningar som resultat. Placering av ett it-utrymme under mark (t.ex. i källare) är olämpligt, speciellt om risker finns för att närliggande vattendrag svämmar över.

It-utrymmen ska under optimala förutsättningar helst placeras ovan markplan, mitt i en fastighet och ska inte angränsa till det yttre skalskyddet. Alla utrymmen utanför it-utrymmets omslutningsyta ska tillhöra en inre säkerhetszon och förvaring av brännbart eller brandfarligt material i närheten ska undvikas.Ett it-utrymme ska placeras så långt ifrån alla vätskeinstallationer i fastigheten som möjligt.

### 2.1.1 Nytt eller gammalt?

Oavsett om en verksamhet bygger en ny fastighet, väljer att flytta till en ny adress eller bygger om i befintliga lokaler brukar placering diskuteras flitigt. Om man bygger nytt eller utför en omfattande renovering har man ofta större möjligheter

att påverka var it-utrymmen ska placeras eftersom infrastrukturen blir ny eller byts ut. Men om en verksamhet flyttar till ny adress, existerar det kanske redan flera it-utrymmen som redan har en fast placering. Ett projekt för att omlokalisera ett eller kanske alla it-utrymmen kan vara svårt att motivera, både praktiskt och ur kostnadshänseende eftersom förändringar av it-utrymmens infrastruktur normalt kräver stora insatser.

Datorhallen hos en verksamhet i norra Sverige var placerad under markplan i en kontorsfastighet. Hallen, som för övrigt var en robust konstruktion, angränsade till en av fastighetens ytterväggar. I marken utanför ytterväggen fanns en av kommunens huvudledningar för färskvatten. Då denna ledning brast, öppnades ett hål i datorhallens vägg och hallen fylldes delvis med vatten, lera och grus. Verksamheten hade varit ovetande om denna risk när hallens placering beslutades flera år tidigare.

### 2.1.2 Analysera och kartlägga

Riskanalysen är ett nödvändigt verktyg när en verksamhet överväger placering. Det är viktigt att denna analys görs tidigt i alla projekt som involverar it-utrymmen eftersom det kan bli mycket kostsamt att vidta åtgärder för riskreducering i efterhand. I riskanalysarbetet är det viktigt att involvera expertis från olika områden, t.ex. fastighetsansvariga, brandexperter, personer med kännedom om geografiska förhållanden, experter på it-miljöer och it-verksamheten.[6]

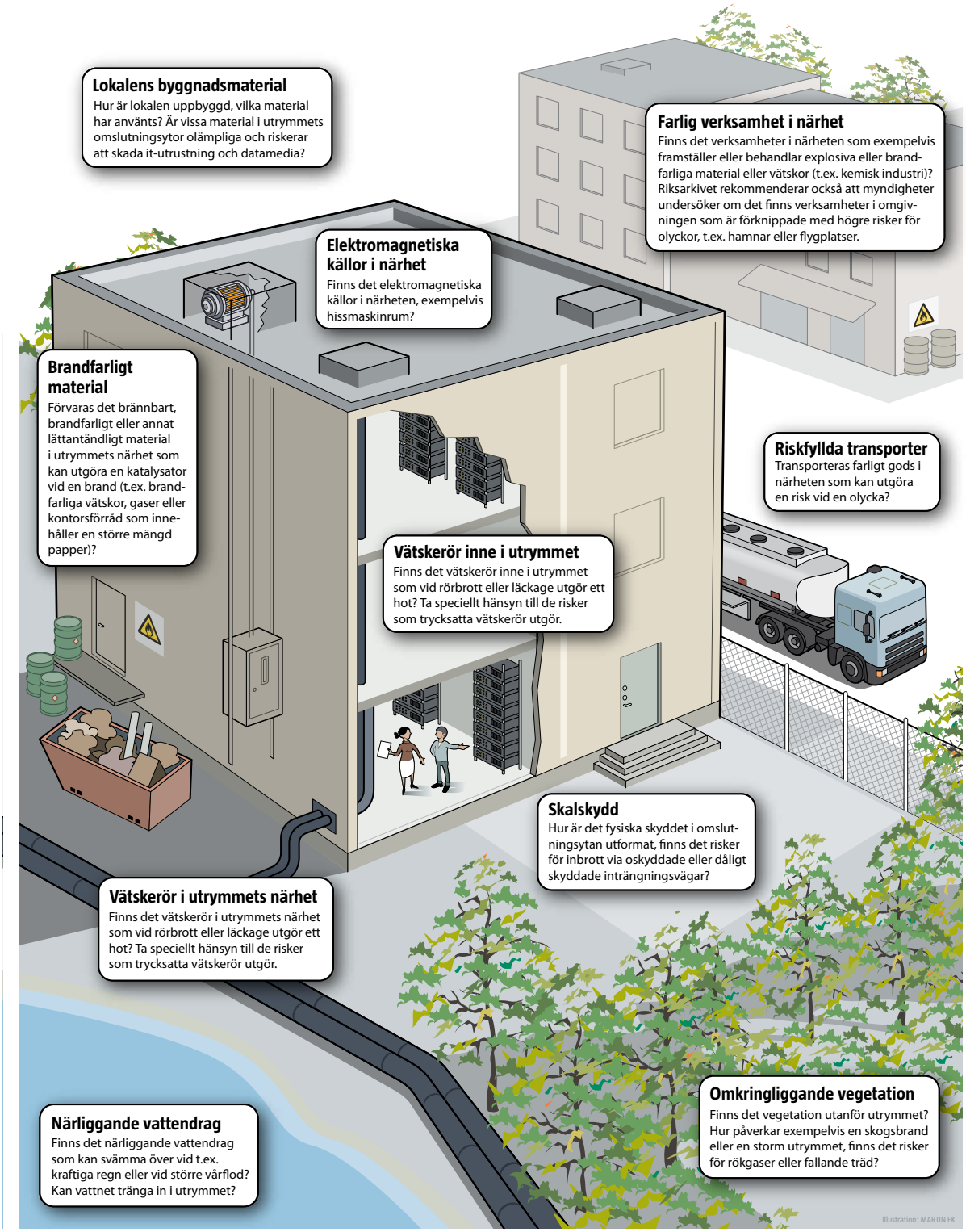
En verksamhet i mellersta Sverige tog beslut efter genomförd riskanalys att omlokalisera sina datorhallar eftersom riskerna för omkringliggande incidenter bedömdes alltför höga. Konsekvenserna av, som i detta fall avsåg inträngande av vatten, skulle bli alltför omfattande och kunna äventyra verksamheten. Kostnaderna för omlokalisering blev omfattande. Hade riskanalysen genomförts initialt, hade stora besparingar gjorts.

Riskanalysen bör ha ett helhetsperspektiv på placeringen av it-utrymmen och framförallt bedöma hot i närliggande områden, i fastigheten och det tilltänkta utrymmet. Nedan följer några områden som bör inkluderas i en analys. Flera av de hot som nämns nedan kan utgöra oacceptabla risker för en verksamhet. Det kan dock vara möjligt att reducera riskerna genom olika åtgärder.

6. Riksarkivet har utfärdat föreskrifter som förbjuder myndigheter att använda lokal som är registrerad som skyddsrum för förvaring av arkiv (RA-FS 2013:4, 4 kap. 2 §).

# It-utrymme

Faktorer som bör analyseras och riskbedömas vid lokalisering av it-utrymmen:




*Figur 1.*

Var med tidigt i planeringen av nya lokaler, ny fastighet, ombyggnationer eller liknande aktiviteter och påverka placeringen av it-utrymmen. Detta gäller alla typer av utrymmen, men är mer viktigt för utrymmen med stora mängder it-utrustning. Med en genomtänkt placering kan riskerna minskas.

### 2.1.3 Skyddsåtgärder vid befintlig placering

Den vanligaste situationen för landets alla företag och organisationer är trots allt relativt statisk. Man har redan lokaliserat ut sina it-utrymmen eller mer vanligt, man har ”ärvt” en befintlig infrastruktur. Det är relativt vanligt att begränsningar i befintliga lokaler har ”tvingat” fram situationen med it-utrymmenas placering, även om denna är långt ifrån optimal ur ett säkerhetsperspektiv. Men även om placeringen inte är optimal, är det ofta möjligt att öka säkerheten med enskilda säkerhetshöjande insatser.

Riskanalysen tillsammans med informationsklassningen är våra viktigaste verktyg för att kunna genomföra säkerhetshöjande åtgärder. Och även en ganska hopplös situation kan med rätt åtgärder ofta vändas till något positivt. Även om man t.ex. har stora problem med inträngande vätska, kan man minska riskerna genom att införa bättre skydd för evakuering av vätska via brunnar eller pumpanordningar. Har en verksamhet problem med återkommande inbrottsförsök kan man stärka inbrottsskyddet och exempelvis öka bevakningen. Kanske kan man välja att omlokalisera delar av sina it-system till en plats som har bättre förutsättningar.

## 2.2 Uppbyggnad, konstruktion och skalskydd

Nästa nivå av skydd efter en bra placering är att datorhallen har en robust konstruktion för att kunna motstå incidenter både utanför och inne i utrymmet. De hot som är relevanta för själva konstruktionen är framförallt skydd mot fysisk åverkan som inbrott, skydd mot brand samt skydd mot miljöpåverkande incidenter i lokalens närhet.

### 2.2.1 Skalskydd

Skalskydd är den gräns i ett utrymme, lokal eller fastighet som har ett fysiskt skydd vilket försvårar forcering och obehörigt tillträde. Utrymmen som förvarar värdefull och känslig elektronisk utrustning som it-utrymmen ska alltid förses med ett skalskydd som möter relevanta hot och omvärldskrav. Uppdelning av skalskydd görs i mekaniskt skydd, elektroniskt skydd och bevakning. Ett första steg är dock att överväga om olika säkerhetszoner kan skapas.

### 2.2.2 Säkerhetszoner

Genom att använda skyddsbarriärer i en fastighet kan en verksamhet nå ytterligare skydd. Om en skyddsbarriär forceras behöver detta inte betyda att säkerheten för den resurs som ska skyddas äventyras omedelbart. Denna typ av indelning brukar benämnas skyddsområden, zoner eller säkerhetszoner. En säkerhetszon kan vara ett låsbart utrymme, ett eller flera områden som omges av en obruten intern fysisk skyddsbarriär eller liknande.

En säkerhetszon har också en typ, inre eller yttre säkerhetszon. En yttre säkerhetszon gränsar till ett område där ingen kontroll av behörighet sker. Utanför en yttre säkerhetszon har vanligen allmänheten tillträde. En inre säkerhetszon gränsar endast till områden av samma typ eller till en yttre säkerhetszon.

En smart placering av en arbetsplats, t.ex. en reception, kan bilda en skyddsbarriär. Verksamheten kan på detta relativt enkla sätt nå en högre kontroll av tillträde till känsliga utrymmen.

Samtliga typer av it-utrymmen bör vara egna inre säkerhetszoner, vilket medför att tillträde till utrymmet alltid ska kunna kontrolleras. Generellt bör alla typer av it-utrymmen placeras i inre säkerhetszoner. På detta sätt kan man utnyttja de skydd som finns i omkringliggande områden, vilket i sin tur kan minska behovet av skydd för det enskilda it-utrymmet. Om man inte har något val och tvingas placera ett it-utrymme i en yttre säkerhetszon, bör man vara beredd på att kompletteringar i lokalens mekaniska skydd sannolikt är nödvändiga. Använd riskanalysen som verktyg för att avgöra behoven av skydd.

Många verksamheter använder också säkerhetszoner inne i it-utrymmen. Vanligen förkommer detta i större it-utrymmen av typen datorhallar men kan även finnas i mindre utrymmen för korskopplingar och kommunikationsnoder. Säkerhetszoner konstrueras oftast med gallerväggar och gallerdörrar och sektionerar på så sätt tillträden. Kartlägg vilka it-system och vilken information som eventuellt kräver dessa skydd. Tänk på att eventuellt placera de mest skyddsvärda resurserna längst in i ett it-utrymme för att undvika att behöva tillåta ”obehöriga” passager. Skåp, stativ och rack kan också utgöra egna säkerhetszoner om dessa förses med lås.

***Bild 1.*** *Säkerhetszoner inne i it-utrymme med gallerväggar.*

Större it-utrymmen av typ datorhallar kan med fördel också förses med en extra säkerhetszon i inpasseringen, en säkerhetssluss. Genom en säkerhetssluss minskar man it-utrymmets exponering mot omkringliggande områden. Det finns också en praktisk fördel med användning av en sluss. Innanför slussen kan dokumentation och reservdelar förvaras. Personalen kan samtidigt få ytor för underhåll och teknisk administration. Miljön inne i ett it-utrymme är ofta obekväm att arbeta i.

### 2.2.3 Mekaniskt skydd

Det mekaniska skyddet utförs i utrymmets omslutningsytor. I omslutningsytan ingår tak, väggar, golv samt dörrar, portar, luckor och fönster med tillhörande lås- och reglingsanordningar. Denna typ av skydd syftar till att hindra att en inkräktare via någon typ av mekanisk forcering, våld eller användning av brytverktyg får tillträde. Vanliga typer av skydd inom detta område är förstärkningar av konstruktioner som exempelvis förstärkta låsförreglingar, ståldörrar, galler eller stålplåt i väggar, tak eller golv.

Ju kraftigare mekaniskt skydd en lokal är utrustad med, desto svårare ska den vara att forcera. Normalt brukar denna svårighetsgrad vara angiven i lokalens skyddsklass. Skyddsklassen ökar med omfattningen och styrkan i det mekaniska skyddet.

**Skyddsklasser**

I Sverige används vanligtvis tre skyddsklasser för mekaniskt skydd. Dessa skyddsklasser är utgivna av Stöldskyddsföreningen (SSF) och finns i ett regelverk som benämns SSF 200, Regler för mekaniskt inbrottsskydd. Externa kravställare såsom myndigheter och försäkringsbolag hänvisar ofta till detta regelverk. Motsvarande regelverk finns i andra länder. Skyddsklasserna i SSF 200 relaterar egentligen till värdet som man avser att skydda. Definitionen av värde är framförallt ekonomisk ur ett försäkringsperspektiv men andra typer av värden är också tillämpliga. Förenklat kan detta uttryckas som att skyddsklass 1 beskriver mekaniskt skydd för resurser av mindre värde, medan skyddsklass 3 är tillämplig för mekaniskt skydd av resurser av stort värde.

Läs mer om mekaniska skydd på *www.stoldskyddsforeningen.se.*

Kraven för ett utrymmes omslutningsyta gäller upp till fyra meter över markplan eller ståplan (exempelvis en avsats utanpå fastigheten).

Övergripande innebär de tre skyddsklasserna i SSF 200[7]:

- **Skyddsklass 1**
  Omslutningsytan ska vara utförd med betong, sten eller lättbetong. Förstärkta regelkonstruktioner med exempelvis skivbeklädnad eller tunn stålplåt kan också godtas.

7. För mer detaljerad beskrivning se konstruktionsregler i SSF200. www.stoldskyddsforeningen.se

- **Skyddsklass 2**
  Omslutningsytan ska vara betonggjuten eller murad. Stålplåt mellan dubbla byggskivor och som skarvas och fästs i reglar kan också godtas. I regel krävs kraftigare skivor och tjockare stålplåt än skyddsklass 1.
- **Skyddsklass 3**
  Omslutningsytan ska vara betonggjuten eller murad. Stålplåt krävs vanligen på båda sidor av en förstärkt regelkonstruktion. Enkel stålplåt kan tillåtas om förstärkningar sker och specifika montage tillämpas.

Skyddsklass 1 är generellt inte tillämplig för it-utrymmen eftersom värdet på skyddade resurser är relativt högt. Skyddsklass 2 och 3 motsvarar bättre de mekaniska skydd ett it-utrymme har behov av.

För att kunna avgöra vilken av skyddsklasserna 2 eller 3 som är tillämpliga för en verksamhet ska utöver informationsklassningen en riskanalys alltid göras. Generellt bör alltid skyddsklass 2 användas som utgångspunkt för alla typer av it-utrymmen, men skyddsklass 3 kan vara aktuell om omständigheter existerar som underlättar forcering, t.ex. utrymmets placering.

SSF 200:s skyddsklasser anger betong som lämpligt material för mekaniskt skydd i omslutningsytor. Armerad betong är svårforcerat och lämpligt som mekaniskt skydd, men som material i omslutningsytan hos ett it-utrymme är det olämpligt eftersom materialet binder vatten. Vid en brand kan vattnet förångas och skada utrustningen i hallen.

### Dörrar

För att en skyddsklass ska upprätthållas för ett utrymme krävs också att dörrarna är mekaniskt skyddade via ett inbrottsskydd. I den europeiska standarden SS EN 1627 anges svårighetsgraden att forcera en dörr i motståndsklassning. Det finns 6 motståndsklasser, SSF 200 skyddsklass 2 motsvaras av motståndsklass 3 och skyddsklass 3 motsvaras av motståndsklass 4.

### Dörrlås

Dörrlås indelas i fem klasser efter klassningens inbrottsskyddande funktion. Kraven på lås finns i den svenska standarden SS 3522. Ju högre klassning, desto svårare att forcera låset. I SSF 200 framgår att det för en godkänd låsenhet i skyddsklass 1 och 2 krävs ett lås av låsklass 3 eller högre medan det i skyddsklass 3 krävs två sådana låsenheter.

### Fönster

Fönster och andra glaspartier ska generellt undvikas i it-utrymmen eftersom de normalt medför en försvagning av det mekaniska skyddet i omslutningsytan (även utrymmets brandskydd då brandskyddsklassat glas måste användas). Om det ändå finns fönster ska dessa förses med inkrypningsskydd, exempelvis galler[8].

8. Riksarkivet tillåter inte fönster vid nybyggnation av en arkivlokal. Om det finns fönster i en befintlig lokal som anpassas till arkivlokal ska fönsteröppningen byggas igen eller kompletteras med brandklassad fönsterlucka som är brandgastät (RA-FS 2013:4, 5 kap. 1 §).

**Övriga öppningar i omslutningsytan**
Andra typer av öppningar eller hål i ett it-utrymmes omslutningsyta såsom exempelvis luckor, ventilationstrummor eller liknande ska generellt undvikas. Om denna typ av öppningar ändå existerar ger SSF 200 vägledning i hur dessa ska skyddas med exempelvis lås, galler eller andra typer av förstärkningar eller inkrypningsskydd.

> Försök att undvika alla typer av öppningar i en omslutningsyta. Begränsa typen av öppning till dörrar som kan förstärkas. Andra typer av öppningar försvagar normalt det mekaniska skyddet.

### 2.2.4 Elektroniska skydd

Det elektroniska skyddet utförs normalt i utrymmets skalskyddsgräns och kompletterar det mekaniska skyddet. Vanligtvis utgörs det elektroniska skyddet av ett inbrottslarm samt andra detektorer för att påkalla uppmärksamhet, exempelvis kameraövervakning. Även passersystem kan räknas till elektroniska skydd (behandlas i kapitel 2.3.3).

**Inbrottslarm**
Likt det mekaniska skyddet delas anläggningar för inbrottslarm in i olika klasser. Högre klassning betyder generellt att larmet är svårare att forcera eller störa ut. Idag ges regler för inbrottslarm ut av Svenska Stöldskyddsföreningen (SSF) och anger de krav försäkringsbolag och andra kravställare ställer på utrustning, projektering och installation. En inbrottslarmanläggning utformas med fyra typer av skydd:

- **Skalskydd**
  Larmet utgör ett skydd i lokalens omslutningsytor. Vanliga typer av detektorer är magnetkontakter, glasdetektorer, vibrationsdetektorer och aktiva IR–detektorer.
- **Försåtsskydd**
  Denna skyddstyp används för att skydda strategiska passager inne i lokaler och ska larma när en inkräktare passerar skyddet. För försåtskyddet används ofta rörelsedetektorer.
- **Volymskydd**
  Larmet är anpassat till ett specifikt utrymme och är utfört på ett sådant sätt att det utlöses när en förändring sker inom utrymmet. Flera typer av detektorer kan användas.
- **Punktskydd**
  Används vanligen för att skydda specifika objekt som exempelvis kassaskåp, stativ/rack eller annan värdeförvaring. Vanligtvis används vibrationsdetektorer för detta skydd.

Reglerna för inbrottslarm beskrivs i SSF:s regelverk SSF 130 Projektering och installation av inbrottslarmanläggning. I SSF 130 återfinns fyra larmklasser och dessa innebär övergripande:

- **Larmklass 1**
  Larmanläggningen har endast försåtsskydd och får till- och frånkopplas genom låsförbikopplare vid ingången till utrymmet.

- **Larmklass 2**
  Larmanläggningen övervakar utrymmets skalskydd i kombination med invändigt försåtsskydd. Larmanläggningens funktion ska också vara övervakad. Till- och frånkoppling sker via manöverpanel.
- **Larmklass 3**
  Krav som larmklass 2, men utrymmets hela yta ska övervakas (volymskydd), utantaget vissa mindre ytor. Själva larmöverföringen (t.ex. till bevakningsföretag/väktare) ska också vara övervakad. Högre krav på teknik i till- och frånkoppling.
- **Larmklass 4**
  Krav som larmklass 3, men utrymmets hela yta ska övervakas (volymskydd), inga undantag för mindre ytor. Högre krav på teknik i till- och frånkoppling samt även för placeringen av manöverpanelen.

För it-utrymmen är samtliga klasser aktuella, men kravställare fokuserar vanligen på larmklass 2 och 3 eftersom värdet av skyddade resurser är högt. Informationsklassning och riskanalys är återigen viktiga instrument för att avgöra vilket behov av skydd verksamheten har. Visar riskanalyser att det finns förhöjd risk för inbrott, ska alltid de högre larmklasserna tillämpas. Typen av it-utrymme samt mängderna utrustning som förvaras i lokalen har också betydelse. Lokaler med större mängd it-utrustningar ska alltid tillämpa minst larmklass 2 vid installation av en larmanläggning.

> Läs vidare i den svenska standarden SS-EN 50131-1 för installationer av inbrottslarmanläggningar och även Stöldskyddsföreningens regelverk SSF 1014 som hanterar materiel för inbrottslarm.

### 2.2.5 Bevakning

Ytterligare en del av skalskyddet är bevakning. Normalt sker bevakning av lokaler med antingen personella resurser (väktare) eller med kameror. En kombination av dessa båda typer är vanligt. Vissa verksamheter har personal på plats för bevakning dygnet runt medan andra verksamheter har en externt kontrakterad bevakningsorganisation som endast agerar vid larm. Många verksamheter har också rondering av lokaler om exempelvis personella resurser saknas utanför kontorstid.

> Tänk på att det är viktigt att överföra den egna verksamhetens säkerhetsregler och rutiner för säkerhet till den bevakande organisationen. Det är vanligt att denna kunskapsöverföring inte sker i tillräcklig omfattning och därför orsakar incidenter.

Eftersom bevakningsorganisationen vanligen är den organisation som tar emot larm från en övervakad verksamhet är det också denna organisation som agerar på larm. Vilka typer av larm och hur den bevakande organisationen ska agera vid händelser bestäms i ett avtal med organisationen.

It-utrymmen bör bevakas och inkluderas i bevakningsorganisationens ronderingar. Många it-utrymmen är försedda med olika typer av driftlarm som också kan skickas till en bevakningsorganisation. Om driftlarm ska hanteras av en bevakningsorganisation är det mycket viktigt att det finns tydliga rutiner kopplade till varje larmtyp. Vilken nivå av skydd i bevakningen som krävs beslutar en verksamhet genom riskanalys och klassning av information.

### 2.2.6 Skydd mot elektromagnetisk strålning

En Faradays bur är ett utrymme som är avskärmat från elektriska fält och elektromagnetisk strålning genom ett elektriskt ledande hölje. Har man som verksamhet krav på skydd mot elektromagnetisk strålning ska man överväga att införa detta skydd i it-utrymmen. Normalt gäller dessa krav endast verksamheter som hanterar extremt känslig information.

RÖS (Röjande signaler)-skydd är ytterligare en typ av skydd mot elektromagnetisk strålning. Kraven för ett komplett RÖS-skydd är dock mer omfattande än för ett ”vanligt” EMP (elektromagnetisk puls)-skydd med en Faradays bur.

## 2.3 Tillträdesskydd och passersystem

För att förhindra att negativa händelser sker genom att obehöriga kan nå fysiskt tillträde till it-utrustning och datamedia ska tillträdet begränsas. Risker finns annars att informationens tillgänglighet och konfidentialitet påverkas. Det är grundläggande att begränsa tillträdet i en verksamhets it-utrymmen till den grupp medarbetare som har ett fastställt behov.

I många verksamheter har också väktare, servicetekniker, fastighetsansvariga, städare eller andra liknande grupper tillträde till it-utrymmen. Dessa personalgrupper är ofta inte anställda i den egna verksamheten och lyder därför under andra anställningsregler. Även om kontraktstyrda relationer finns behöver det inte betyda att ansvar och befogenheter regleras på samma sätt. Dessa externa personalgrupper bör därför inte ha fritt eller oreglerat tillträde till it-utrymmen om det inte är absolut nödvändigt.

> Det är viktigt att ha kontroll över vem som har tillträde till datorhallar och andra tekniska utrymmen där it-utrustning och datamedia förvaras.

### 2.3.1 Olika typer av tillträdesskydd

Det finns flera sätt att begränsa tillträde till en verksamhets it-utrymmen. Följande skydd och systemlösningar är vanliga idag:

- **Mekaniska lås (låssystem)**
  Vanliga fysiska lås som låses med en fysisk nyckel.
- **Kodlås**
  Elektroniska lås som öppnas med en sifferkombination.
- **Passersystem (passerkontrollsystem)**
  Ett tekniskt system med behörighetsfunktioner som styr och manövrerar elektroniska lås.

Mekaniska lås och kodlås är endast lämpliga för mindre typer av utrymmen med en begränsad mängd utrustning eftersom nivån i skyddet generellt är låg och det kan vara svårt att kontrollera vem som passerar (bristande spårbarhet). För större typer av it-utrymmen med stora mängder utrustning, ska ett passersystem användas. Använd fastighetens befintliga passersystem även för samtliga it-utrymmen.

Observera att även om man använder ett passersystem är vanligen samtliga passager utrustade med ett mekaniskt lås som går att låsa upp med en nyckel. Detta är nödvändigt i händelse av att passersystemet upphör att fungera.

Hos en verksamhet i västra Sverige startade en brand i en datorhall. Eftersom hallen var utrustad med fönster uppmärksammade personalen branden tidigt och hämtade en handbrandsläckare. När man försökte använda passerkort och kod för inpassage till hallen låstes inte dörren upp. Orsaken var att kablarna till manöverpanelen hade brunnit av. Man försökte då hitta nyckeln till det mekaniska låset. Nyckeln hittades till slut och man kunde låsa upp och släcka branden, men skadorna i utrymmet hade avsevärt förvärrats under den tid det tog att hitta nyckeln. Idag har minst en medarbetare i tjänst en fysisk nyckel till datorhallen på sin nyckelknippa.

Den låscylinder som används i det mekaniska låset till samtliga it-utrymmen bör ingå i en egen behörighetsgrupp. Det ska krävas nyckel i denna behörighetsgrupp eller en huvudnyckel för att mekaniskt låsa upp låset.

### 2.3.2 Förutsättningar för identifikation

Nivåer av tillträdesskydd för in och utpassering till ett utrymme baseras på tre identifikationsfaktorer:

- **Något man vet**
  Utgörs normalt av en sifferkombination (t.ex. PIN-kod).
- **Något man har**
  Är vanligen någon form av fysisk enhet, såsom passerkort eller nyckel-tagg.
- **Något man är**
  Kontroll av en unik personlig egenskap (biometrisk) såsom fingeravtryck, röst eller retina-mönster (i ögonen).

Lägsta nivån av skydd fås då man utnyttjar en av identifikationsfaktorerna ovan enskilt. Detta brukar normalt kallas för en-faktoridentifikation. Vanliga former av en-faktoridentifikation vid passage är fysisk nyckel (mekanisk nyckel) eller nyckeltagg. Spårbarhet vid en-faktoridentifikation härleds via en kontroll (t.ex. register) över vilka som har nyckel eller tagg, men själva identifikationen sker egentligen mot den fysiska enheten. Metoden identifierar egentligen inte personen som använder enheten i låset (undantaget om en biometrisk faktor används).

I nästa nivå kombineras två identifikationsfaktorer. Den vanligaste kombinationen är en sifferkod (något man vet) tillsammans med ett passerkort (något man har). Andra varianter är också möjliga, t.ex. sifferkod tillsammans med fingeravtryck osv. Via två-faktoridentifikation ökar spårbarheten eftersom det är möjligt att identifiera personen som passerar. Denna typ av identifikation är den vanligaste vid tillträden till utrymmen med känslig information och utrustning.


***Bild 2.** Inpassering med två-faktoridentifikation, tagg och sifferkod.*

Använder man alla tre identifikationsfaktorerna tillsammans når man ytterligare en nivå av skydd. För verksamheter med extremt känsliga it-system och information kan tre-faktoridentifikation vara nödvändigt för passage till it-utrymmen.

Vissa organisationer och företag väljer också att öka skyddsnivån under vissa tider. Under kontorstid använder man en-faktoridentifikation och ökar till två faktorer under kvällar och helger.

Tillträdesskyddet till känsliga utrymmen kan också ytterligare förbättras genom användning av andra tekniska lösningar eller anpassningar i passersystem. Exempel på dessa är:

- **Sluss**
  En sluss kan programmeras i ett passersystem och består då av två passager. Passersystemet styr slussen genom att den ena passagen endast kan öppnas om den andra är stängd och låst. En sluss begränsar den möjliga ytan och spridningen hos en incident.
- **En-personssluss**
  En en-personssluss är en variant av sluss och kallas också för mantrap. Funktionen är likadan som hos en vanlig sluss med skillnaden att passagen endast

tillåter en person åt gången. Slussen kan också förses med ytterligare säkerhetsteknik, exempelvis teknik för att upptäcka införsel av otillåten materiel. En en-personssluss ger generellt ökad säkerhet i en passage.

- **Anti-passback**
  Detta är en teknik som kan programmeras i ett passersystem och förhindrar att flera personer gör en inpassering med samma fysiska enhet (t.ex. nyckel-tagg). Därför används identifikation både vid in- och utpassering. Har en person exempelvis gått in i en datorhall, måste samma person göra en korrekt utpassering från hallen innan passersystemet kommer att tillåta en ny inpassering. Anti-passback minskar risken för missbruk av passager i allmänhet.

Det är vanligt att verksamheter kräver att alla tillträden till it-utrymmen för servicepersonal ska övervakas kontinuerligt. Anti-passback kan då användas för att ”tvinga” personal att kontinuerligt övervaka arbetet. Om en servicetekniker släpps in i en datorhall med personalens nyckel-tagg, måste samma person följa med in för att serviceteknikern ska kunna komma ut. Missbruk elimineras kanske inte, men risken minskar.

### 2.3.3 Passersystem

Definitionen av ett passersystem (även kallat passerkontrollsystem) är ett tekniskt system som styr och manövrerar elektroniska lås. De största skillnaderna mot traditionella mekaniska lås är att man får en förenklad administration samt en bättre spårbarhet. Eftersom man använder elektroniska nycklar (nyckel-taggar, passerkort eller liknande) kan man garantera att inga dubbletter av nycklar finns. Förutom spårbarhet i passager genom loggning kan man enkelt skapa behörighetszoner, olika tidprogram vilka begränsar tillträden eller ökar antalet identifikationsfaktorer vissa tider på dygnet m.m. Dessutom kan man enkelt spärra ut borttappade nycklar vilket ger en avsevärd besparing jämfört med samma moment i ett traditionellt låssystem. Passersystem idag har ofta öppna gränssnitt vilket även möjliggör integration med andra system som inbrottslarm, videoövervakning, registrering av arbetstid eller överordnade system som integrerar flera funktioner.

Den norm som vanligen förekommer i svenska kravställningar för installationer av passersystem är utgiven av Svenska Stöldskyddsföreningen, SSF 210:2[9] Projektering och installation - Elektromekanisk låsanläggning.

I Sverige finns många passersystem på marknaden. Oavsett vilken produkt man väljer stödjer dessa alltid olika typer och fabrikat av läsare som exempelvis kortläsare, beröringsfria eller biometriska läsare.

9. Läs mer om SSF 210:2 på www.stoldskyddsforeningen.se

*Bild 3. Nyckelbrickor kan förses med beröringsfri avläsning.*

Den vanligaste elektroniska nyckeln i ett passersystem är idag passerkort eller nyckel-tagg, även om möjlighet finns att ansluta andra avläsningar av exempelvis biometriska faktorer. Magnetkort är en äldre teknik som också fortfarande används i Sverige, men som man bör försöka fasa ut eftersom korten kan vara lätta att kopiera. Den vanligaste tekniken idag är enheter som nyckelbrickor (taggar), smartcard eller andra kort som förses med en beröringsfri avläsning, vanligen RFID[10]. Dessa typer av enheter är svårare att kopiera och erbjuder en bättre säkerhet. Det finns också varianter som använder kryptering för ytterligare säkerhet. Vissa varianter av dessa har dock visat sig ha brister som gör dessa möjliga att kopiera och missbruka. Anlita därför alltid expertis på området innan ni beslutar om val av passersystem och teknik.

Innan ni beslutar om ett passersystem, försök att konsultera oberoende expertis inom området. Utvärdera olika potentiella leverantörer och jämför lösningar och teknik. Det är fortfarande vanligt med en för övergripande och otydlig kravställning inom området.

Passersystem till it-utrymmen ska alltid ingå i en egen behörighetszon. Endast den grupp av personer som har uttalade behov av tillträde till en verksamhets it-utrymmen ska ingå i en separat behörighetsgrupp. Denna behörighetsgrupp ska vara den enda som har tillträde till it-utrymmen. Använd alltid minst två identifikationsfaktorer för tillträde och kontrollera att alla passager till -utrymmen loggas i passersystemet.

10. RFID, Radio Frequency Identification

### 2.3.4 Andra typer av tillträdesskydd

Andra typer av tillträdesskydd till it-utrymmen som kan införas för att förbättra nivån på skyddet inkluderar följande:

- **Kameraövervakning (CCTV[11])**
  Passagen till ett it-utrymme samt it-utrymmet i sig kan båda förses med övervakningskamera. Används en sluss kan man använda en övervakningskamera för att även optiskt verifiera ett tillträde. Kameraövervakning kan integreras med ett passagesystem. Används någon form av överordnat system kan man exempelvis få en passagebegäran att starta en associerad kamera. Många verksamheter använder dock endast passiv kameraövervakning (dvs. bilder spelas in) för att man i efterhand ska kunna kontrollera eventuella obehöriga passager. Integrerad kameraövervakning kräver ofta ett helt system, medan passiv kameraövervakning kan uppnås med enskilda komponenter. **Kameraövervakning måste följa kameraövervakningslagen**[12] så att den inte inkräktar på den personliga integriteten.

***Bild 4.*** *Kameraövervakad in- och utpassering vid ett it-utrymme*

Kameraövervakning kan kräva tillstånd och samverkan bör ske med arbetstagarorganisationer vid kameraövervakning som kan inverka på anställdas integritet.

11. CCTV, Closed Circuit Television, engelsk benämning på övervakningskamerasystem
12. www.datainspektionen.se/lagar-och-regler/kameraovervakningslagen/

- **Reception/bemannad passage**
  En reception eller annan typ av bemannad passagekontroll kan behövas för verksamheter som har extremt känslig information eller känsliga it-system.
- **Sektioner i it-utrymmet**
  Passagesystem kan användas för att skapa separata sektioner i ett it-utrymme. Normalt installeras gallersektioner för att skilja utrustning åt, men passagesystemet kan även anslutas att kontrollera tillträde till enskilda skåp/rack eller stativ samt integreras med en inbrottslarmanläggning för att ytterligare öka skyddet.

## 2.4 Brandskydd

En brand i eller i närheten av it-utrymmen kan få mycket allvarliga konsekvenser. Ett tillförlitligt brandskydd är nödvändigt för att minimera risker och skydda de stora ekonomiska värden som finns investerade i en verksamhets informationsresurser.

Det är främst två typer av hot som ska bemötas av ett brandskydd:

- den direkta branden, dvs. brand inuti utrymmet
- den indirekta branden, dvs. en brand utanför utrymmet.

Skydd mot direkt brand utgörs normalt av ett manuellt eller mer vanligt automatiskt släcksystem. Den indirekta branden ska bemötas av brandskyddet i utrymmets omslutningsyta som ska utgöra brandcellsgräns. Det finns också andra anpassade varianter av brandskydd för it-utrustning och datamedia. Dessa kommer att diskuteras senare i kapitlet.

### 2.4.1 Brandbelastning

Begreppet brandbelastning används som ett mått på den sammanlagda värmemängden som frigörs vid en fullständig förbränning av allt brännbart material i ett utrymme, även material i byggnadskonstruktionen. Mer brännbart material medför högre brandbelastning. Begreppet brandbelastning används exempelvis i byggregler för att bestämma brandteknisk klass på brandcellsavskiljande konstruktioner.

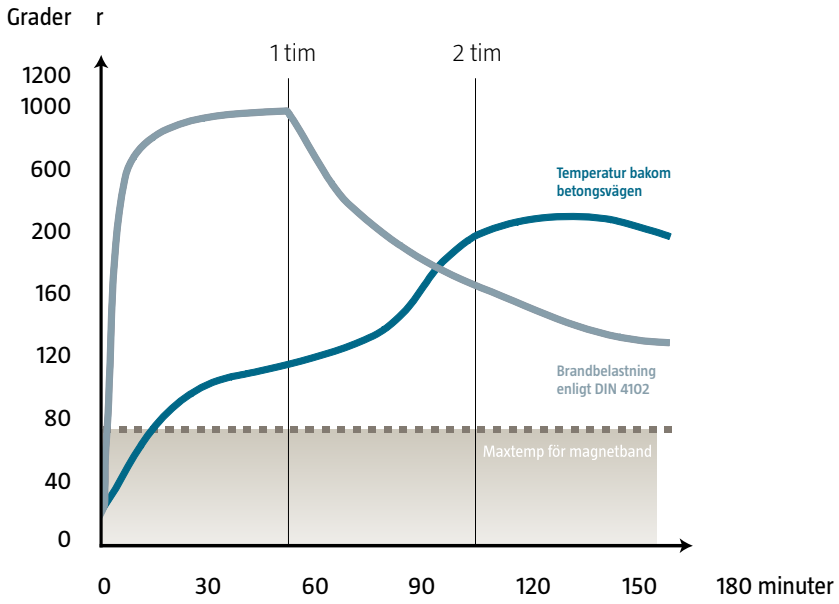
Gemensamt för samtliga skyddsvärda utrymmen är att man ska sträva efter att minska brandbelastningen i närheten av utrymmet. Vanligen sker detta genom att man avlägsnar material som förvaras i närheten eller förbättrar det tekniska brandskyddet i omslutningsytans konstruktion. Brandbelastningen kan också minskas genom andra tekniska åtgärder som exempelvis vattensprinkler utanför det utrymme man avser att skydda.

> Kartlägg risker för indirekta bränder mot it-utrymmen. Många verksamheter gör misstaget att helt fokusera på brandskydd mot den direkta branden. Undvik exempelvis att placera material eller verksamheter i it-utrymmets direkta närhet som kan påskynda eller förvärra en indirekt brand, såsom brandfarliga vätskor eller pappersförråd (ökad brandbelastning). Det är även viktigt att ta hänsyn till risker för en indirekt brand mot den fastighetsdel där it-utrymmet är placerat, exempelvis närliggande vegetation som kan utgöra en risk vid en skogsbrand eller närhet till en typ av verksamhet som innebär brandrisk (exempelvis en färgaffär eller en verkstad). Förstärkt brandskydd kan vara nödvändigt.

### 2.4.2 Den indirekta branden

Vid en indirekt brand är det it-utrymmets omslutningsyta (skalskydd) som ska förhindra skador på it-utrustning och datamedia. Det är inte bara brand mot it-utrymmets omslutningsyta som ska bemötas, utan framförallt skydd mot de rökgaser som den indirekta branden skapar. Ett släckningssystem inuti it-utrymmet skyddar inte it-utrustning och datamedia vid indirekt brand. För att ett brandskydd ska fungera krävs initialt att själva it-utrymmet utgör en egen brandcell. Omkringliggande utrymmen i direkt närhet kan också med fördel utgöra egna brandceller för att hindra brandspridning fram till it-utrymmet.

Bilden nedan visar ett brandförlopp utanför ett it-utrymme där materialet i omslutningsytan är betong. Brandklassen i omslutningsytan begränsar spridningen i 90 minuter (EI-90). Den röda kurvan visar temperaturen utanför utrymmet som når 500–600 grader Celsius inom några minuter. Den gröna kurvan visar temperaturen inne i it-utrymmet. Efter cirka 15 minuter passeras gränsen där toleransvärden för datamedia och it-utrustning överskrids.




***Figur 2.** Schematisk bild över brandförlopp utanför ett it-utrymme.*

Obeklädd betong i väggar, golv och tak kan vara direkt olämpligt i it-miljöer eftersom materialet binder vätska. En brand mot en betongvägg kan medföra att vätska i konstruktionen förångas och släpps ut under högt tryck inuti utrymmet och skadar it-utrustning och datamedia. En möjlig skyddsåtgärd kan vara att bekläda betongen med brandskyddande material. Konsultera expertis inom området för lämpliga materialval. Äldre betongarkiv är av ovanstående orsaker inte lämpliga att använda som it-utrymmen.

### 2.4.3 Brandskyddsklasser

Den norm som för närvarande tillämpas i de nationella byggreglerna är EI-normen. E anger integritet och I isolering i omslutningsytan. EI kan kombineras med ytterligare klassbeteckningar för bärförmåga (R) eller exempelvis C som anger krav på dörrstängning. Beteckningen EI följs alltid av en tidsangivelse som anger hur länge den brandavskiljande konstruktionen förhindrar en brands spridning. EI-30 betyder exempelvis att brandspridning förhindras i 30 minuter, EI-120 betyder 120 minuter. De äldre A-klassningarna är liknande utformade men kan ibland anges i timmar (A1 – 1 timmes skydd, A2 – två timmars skydd)[13].

Tänk på att EI endast anger skydd mot brandspridning och inte tar hänsyn till skydd av it-utrustning och datamedia. Utrustning och datamedia skadas allvarligt vid betydligt lägre temperaturer än de 160–200 grader Celsius som EI-klassningen anger inte ska uppnås inom specificerad tid på den icke brandutsatta sidan.

En annan vanligt förekommande skyddsklass i Sverige är SS/EN-1047. SS/EN1047-1 behandlar skåp/förvaring (säkerhetsskåp) och SS/EN1047-2 behandlar it-utrymmen. Likt EI-normen är SS/EN-1047 en metod för att prova olika typer av motståndsförmåga, bl.a. i brandskyddskonstruktioner. SS/EN-1047 är därför inte formellt en brandklassning även om beteckningen ofta används så. Klassen beskriver inte bara brandskydd utan innehåller även andra prov av gastäthet, vätske- och fuktskydd samt skydd mot magnetisk påverkan (så kallat EMP-skydd). Ett utrymme som uppfyller proven i SS/EN-1047 klassificeras med beteckningen R60/90D (även kallat F90D).

Ett utrymme som är konstruerat enligt SS/EN1047-2 skyddar mot brand och fukt (fukt i form av antingen höga luftfuktighetshalter eller fukt och vattenånga som bildas i samband med brandbekämpning med vatten) samt för översvämning (vatten som tränger in i samband med översvämning eller rörbrott i närheten av utrymmet). Vidare inkluderar normen även skydd mot magnetisk påverkan (skydd mot EMP i samband med åska eller sabotage), enligt principen Faradays bur. SS/EN1047-2 anger också skydd mot gas (gasutsläpp av olika typer, stadsgas eller gasmängder från kyltorn etc.). Även skydd mot sabotage (försök till forcering av väggar eller andra funktioner) enligt SSF 200:3 (eller motsvarande europeisk norm) hanteras.

Ett it-utrymme (typ datorhall) som brandskyddas enligt SS/EN-1047 är oftast 5–10 gånger dyrare än en hall med motsvarande EI-klassning. Gör en noggrann avvägning av skyddsbehovet genom riskanalyser. Men avfärda aldrig en lösning under analys eller projektering bara för att den kostar mer. Det är verksamhetens krav som i huvudsak måste styra valet av brandskydd.

13. Enligt Riksarkivets föreskrifter ska arkivlokalen utföras så att den, vid en brand i angränsande utrymmen, under 120 minuter ger skydd mot skadlig upphettning, brandgas, öppen låga och genombränning. Dörrar, fönsterluckor och portar ska vara brandgastäta. Dörrar ska vara utrustade med automatisk stängare och anslagströskel. Med skadlig upphettning avses normalt för magnetiska databärare och optiska databärare >55 °C (RA-FS 2013:4, 7 kap. 4 §).

Internationellt finns varianter av brandskyddsklasser som liknar de som behandlas ovan. Avsikten i dessa klassningar är dock samma som för de svenska varianterna.

### 2.4.4 Skydd mot den direkta branden

Skydd mot direkt brand i ett it-utrymme kan bestå av handbrandsläckare alternativt ett släckningssystem. Manuella släckningssystem är i Sverige relativt ovanliga och är idag ersatta av automatiska varianter. Eftersom ett utlöst släckningssystem ofta medför stora kostnader är de automatiska släckningssystemen utrustade med ett eget brandlarm bestående av separata detektorer för att identifiera en brand. Dessa detektorer är vanligtvis betydligt känsligare än ”vanliga” traditionella branddetektorer och kan därför tidigt identifiera ett brandförlopp. Det är därför vanligt att man implementerar larmnivåer i brandlarmet, där de första nivåerna (för-larm) endast påkallar uppmärksamhet. För att själva släckningssystemet ska aktiveras krävs en högre larmnivå. Automatiska släcksystem har även en manuell aktivering placerad utanför det skyddade objektet.

### 2.4.5 Brandlarm och branddetektorer

Det finns olika typer av branddetektorer på marknaden såsom värmedetektor, rökdetektor (optiska eller joniserande) samt flamdetektor. Den vanligaste förkommande typen är optiska rökdetektorer[14].

***Bild 5.*** *Optisk rökdetektor monterad i tak.*

14. Riksarkivet kräver att arkivlokalen ska vara utrustad med ett automatiskt brandlarm som vidarebefordrar larm till en bemannad plats. Detektorer ska finnas såväl i arkivlokalen som i till arkivlokalen angränsande brandceller som myndigheten (organisationen) förfogar över (RA-FS 2013:4, 7 kap. 15 §).


BRANDLARM
UTRYM SNARAST
ARGONITE UTLÖST
UTRYM OMEDELBART
314426
NORMAL
STYR SLÄCKANLÄGGNING

I it-utrymmen är det vanligt att kylaggregat orsakar en kraftig luftcirkulation. Traditionella branddetektorer som rökdetektorer kan hindras att fungera optimalt eftersom en viss koncentration rök krävs för att detektorn ska lösa ut. Höga lufthastigheter kan medföra att rök späds ut och larm uteblir. Ett enkelt prov kan göras genom att hålla ett tunt A4-papper bredvid en rökdetektor. Om pappret fladdrar fram och tillbaka kommer sannolikt rökdetektorn att upptäcka en brand relativt sent.

I it-utrymmen används också samplande (aspirerande) detektorer som kontinuerligt suger in luft (vanligen via rörsystem). I ett samplande system analyseras luften och om rökpartiklar eller andra miljöavvikelser upptäcks aktiveras brandlarmet.

Ett samplande brandlarm kan exempelvis upptäcka kablar som har upphettats och aktivera för-larm. Möjligheter till manuella insatser finns och om personal finns på plats kan man kanske undvika att en brand utbryter och att släcksystemet aktiveras. För-larmen kan också användas för att aktivera andra typer av manövrar som exempelvis blixtljus och stänga dörrar eller lufttillförsel.

Den huvudsakliga fördelen med ett samplande system är att brandförlopp kan identifieras tidigt eftersom systemet är relativt okänsligt för luftströmmar. Samplande system aktiverar vanligen brandlarm när röktätheten i utrymmet överstiger 0,8 % och släckmedel släpps med en kort fördröjning för att man ska hinna utrymma lokalen. Vid lägre röktäthet aktiveras olika nivåer av för-larm för att påkalla uppmärksamhet genom exempelvis ljud- och ljussignaler samt meddelande till bevakningsorganisationen.

Om ett samplande system saknas är det relativt vanligt att man installerar flera sektioner som kan bestå av samma detektortyp. För att det automatiska släckningssystemet ska aktiveras krävs att alla sektionerna har löst ut (upptäckt branden).

It-utrymmen kan också vara utrustade med branddetektorer som tillhör fastighetens brandlarm. Om ett eget brandlarm för it-utrymmet används kan detta larm anslutas till fastighetens brandlarm. Var noggrann med hur detta ansluts, man vill sällan att ett för-larm från ett it-utrymme ska aktivera en stor fastighets brandlarm och tillkalla räddningstjänst.

Alla installationer av automatiska brandlarm ska utföras av eller under överinseende av en certifierad anläggarfirma som också utfärdar de handlingar som krävs. Installationen ska utföras enligt Regler för automatisk brandlarmanläggning, SBF 110:6 utgiven av Brandförsvarsföreningen. Försäkringsbolag hänvisar ofta till denna referens. Vana av installationer i it-miljöer och it-utrymmen bör också vara ett krav.

***Bild 6 (till vänster).*** *Släckcentral för samplande brandlarm.*

### 2.4.6 Handbrandsläckare

Även om ett automatiskt släckningssystem existerar ska detta alltid kompletteras med handbrandsläckare. Handbrandsläckarna ska vara avsedda för elektriska bränder och placeras primärt utanför it-utrymmet, men i dess direkta närhet för att enkelt nås av personal vid en skarp situation. Kompletteringar av handbrandsläckare inne i ett it-utrymme kan också göras om detta bedöms som nödvändigt.

Undvik användning av släckmedel i handbrandsläckare som är baserade på vatten, skum eller pulver eftersom dessa kan skada it-utrustning och datamedia. Inga handbrandsläckare i närheten av ett it-utrymme ska innehålla dessa typer av släckmedel. Använd släckmedel utformat för elektriska bränder som exempelvis kolsyra.

### 2.4.7 Automatiska släcksystem

Automatiska släcksystem finns i olika varianter. Men det är framförallt vilken typ av släckmedel som används som skiljer systemen åt. De vanligast förekommande släckmedlen är olika varianter av gas och vatten. Båda typerna av släckmedel påverkar de faktorer som ska existera för att en brand ska kunna uppstå, nämligen tillgång till syre, bränsle och värme.

Undvik traditionella vattenbaserade sprinklersystem (fastighetssystem) i alla typer av it-utrymmen eftersom dessa kan skada it-utrustning och datamedia allvarligt.

#### Gas

Gas som släckmedel förhindrar brand genom att syrehalten i utrymmets luft sänks samt att temperaturen i själva branden sänks. Gasen sänker dock inte syrehalten till en nivå som medför att utrymmet blir farligt att vistas i för människor. Vanligt förekommande gassläckmedel är halotroner, koldioxid, kvävgas eller inerta gaser som inergen, argonite eller novec. En fördel med gas är att släckeffekten ligger kvar i ett utrymme under lång tid och hindrar en brand från att återaktiveras. Ytterligare en fördel är renheten, dvs. att ingen utökad sanering är nödvändig efter en släckt brand. Till nackdelarna hör en relativt högre kostnad samt att stora mängder gas används (gasflaskorna tar mycket utrymme). I och med att stora mängder gas släpps ut (högt tryck) krävs också att ett it-utrymme förses med övertrycksventiler eftersom utrymmets omslutande konstruktion annars kan skadas. Novec har en lägre inblandning på grund av sin kemiska sammansättning, vilket gör att övertrycksspjäll inte behövs och att installationen kräver mindre plats (färre gasflaskor). Gasflaskor kan placeras utanför it-utrymmet.

En verksamhet i sydöstra Sverige drabbades av en brand inne i en datorhall. Släcksystemet (gas) löste ut som planerat och släckte branden. Datorhallen var tyvärr inte utrustad med ett övertrycksspjäll vilket resulterade i att en av väggarna i hallen trycktes ut i korridoren utanför hallen.

***Bild 7 (till vänster).*** *Gasflaskor tillhörande ett automatiskt brandsläckningssystem.*


stängt
öppet

**Halotron**
På marknaden finns också olika halotroner utvecklade från den numera förbjudna gasen halon som gassläckmedel. Vanliga benämningar är t.ex. EX200 eller FM200 och funktionen är densamma som hos inerta gaser. Halotron-utvecklingar är förbjudna i Sverige av miljöskäl men tillåtna inom vissa EU-länder. Det kan också vara möjligt att behålla en äldre anläggning baserad på halon och endast byta typ av gas. Var uppmärksam på att dessa installationer kan kräva speciella tillstånd av kommunala miljöenheter eller liknande, vilka av uppenbara skäl kan belägga installationerna med omfattande avgifter, kontroller och rapporteringsansvar.

Var uppmärksam på att en fastighets bygglovshandlingar kan innehålla krav på vattenbaserade sprinklersystem i samtliga utrymmen. Detta medför att bygglovshandlingarna blir ogiltiga om sprinklersystemet avaktiveras i ett it-utrymme. Ansök därför om förändring i bygglovet vid installation av ett automatiskt släckningssystem i ett it-utrymme.

**Vattendimma**
Ett annat vanligt släckmedel som bl.a. används i it-utrymmen är vattendimma. Vattendimma använder avjoniserat vatten som släckmedel vilket sprids av en drivgas, exempelvis koldioxid. Drivgasen slår sönder vattendropparna och skapar en dimma som sänker temperaturen och kväver en brand. Även om vatten är ett effektivt släckmedel (flera gånger effektivare än vissa gaser) är det olämpligt att använda i it-utrymmen eftersom det medför negativa konsekvenser. En släckt brand (eller att systemet felaktigt har löst ut) kommer att medföra utökade saneringsåtgärder eftersom vatten kan binda sot och andra partiklar. Utrustning kommer att behöva plockas isär och rengöras innan man kan återgå till normal drift. Elektronik i it-utrustning kan också kortslutas, även om vattendimman är avjoniserad.

För ett 10-tal år sedan löste ett släcksystem med vattendimma ut hos en verksamhet i mellersta Sverige. Larm inkom till bevakningsorganisationen eftersom ingen ordinarie personal fanns på plats. Väl på plats konstaterades att en brand hade förhindrats men att miljön i utrymmet var i behov av sanering. Flera veckor efter saneringen började fel uppträda i utrymmets kylanläggning. När kylaggregaten hade tagits isär kunde man konstatera att reparationer var nödvändiga eftersom delar hade skadats av rost. Orsaken var sannolikt vattendimman.

Som angivits ovan har var och en av dessa släckmedel sina för- och nackdelar. När det gäller att bekämpa det direkta brandförloppet är alla effektiva även om skillnader finns mellan olika typer av släckmedel. Vattendimma bör undvikas som släckmedel eftersom skaderisker finns för alla typer av elektrisk eller mekanisk utrustning i it-utrymmet. Halotroner bör undvikas på grund av den negativa miljöpåverkan de medför.

***Bild 8 (till höger).*** *Övertrycksspjäll i ett it-utrymme med Argonite som släckgas.*

### 2.4.8 Sektionera som en del i brandskyddet

Genom att sektionera ett it-utrymme i flera olika delar kan man minska mängden släckmedel som behövs. Varje sektion förses då med en separat detektering och släckmedel skickas endast till den sektion som upptäcker brand.

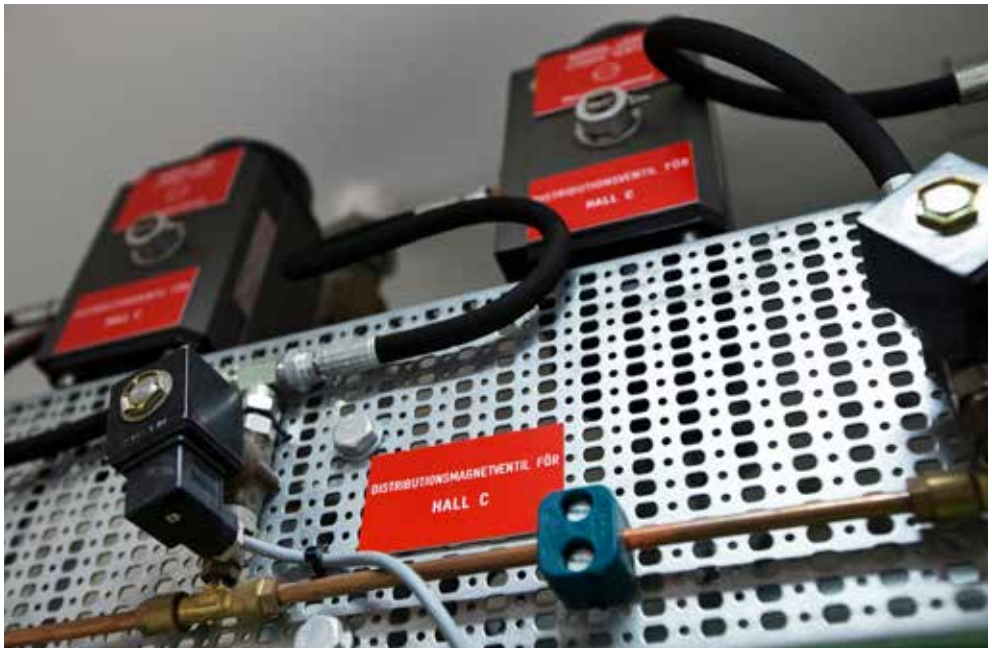



*Bild 9. Utrustning för att fördela släck-gas till separata utrymmen.*

Ytterligare ett alternativ för att öka brandskyddet kan vara att sprida ut it-utrustning och datamedia till flera utrymmen. Avståndet mellan dessa utrymmen bör då vara tillräckligt för att en eventuell brand inte ska påverka samtliga it-utrymmen samtidigt[15].

**Datacontainers**

Om en verksamhet generellt har svårigheter att förbättra brandskyddet hos sina it-utrymmen finns det andra möjligheter. På marknaden finns idag brandskyddade skåp vilka fungerar som en ”mini-datorhall” med egen kyla och andra lämpliga skydd. Dessa skåp benämns vanligen datacontainers.

## 2.5 Miljö och kyla

Den el som it-utrustning förbrukar omvandlas efter hand till värme som måste transporteras bort. Den uppvärmda luften från utrustningen leds vanligtvis genom en värmeväxlare eller värmepump där den kyls ner och sedan återcirkuleras till utrymmet. För mindre utrymmen kan det vara tillräckligt att kyla med utomhusluft, men större it-utrymmen kräver alltid en kylanläggning. Vanligtvis används flera kylaggregat med viss överkapacitet så att temperaturen kan hållas även om ett aggregat går sönder. Om kylningen slutar att fungera kommer temperaturen

15. Enligt Riksarkivets regler får elektrisk arbetsplatsutrustning inte finnas i arkivlokalen. Dessa bör placeras i ett från arkivlokalen brandtekniskt avskilt utrymme, dvs. i en annan brandcell (RA-FS 2013:4, 7 kap. 8 §).

att stiga snabbt. I ett utrymme med stora mängder utrustning kan ökningen vara en grad per minut eller mer. Efter en timme kan temperaturer mellan 80 och 90 grader Celsius nås med allvarliga skador på it-utrustning och datamedia som följd. Det blir dock mer och mer vanligt att it-utrustningar förses med överhettningsskydd som initierar automatisk avstängning.

> Om man mäter temperaturen i sitt it-utrymme ska mätningen ske där utrustningen suger in den kylda luften. Det är på denna plats i it-utrymmet som temperaturen är avgörande, temperaturer på andra platser är inte lika viktiga. Används rack, stativ eller hyllor görs mätningen högt upp i montagen där luften är som varmast eftersom varm luft stiger.

Eftersom miljön i ett it-utrymme är en så vital faktor för att kunna upprätthålla en kontinuerlig it-drift, är larm och övervakning av miljöfaktorer extremt viktigt. Mer om miljölarm och övervakning i kapitel 2.9 Teknisk övervakning och larm.

### 2.5.1 Miljöstörningar och dess effekter

En miljöstörning som medför ökad temperatur i ett it-utrymme kan ha två orsaker, brand eller trasig kylanläggning. Vid en brand ökar temperaturen, luftens relativa luftfuktighet förändras och skadliga (korrosiva) rökgaser uppstår. Om kylanläggningen i ett it-utrymme går sönder, ökar temperaturen och den relativa luftfuktigheten förändras.

Vid en miljöstörning finns det skillnader i tolerans hos it-utrustning och datamedia. Generellt är båda känsliga för störningar och varken it-utrustning eller datamedia kan stå emot heta rökgaser. It-utrustning klarar dock av temperaturökningar något bättre än datamedia. It-utrustning såsom servrar, hubbar, switchar etc. kan skadas allvarligt redan vid 70 grader Celsius och datamedia påverkas redan vid 55 grader.

Är temperaturen för låg eller luftfuktigheten för hög kan kondens skapas som orsakar kortslutningar. Är den relativa luftfuktigheten för låg kan statisk elektricitet byggas upp i it-utrustningens elektronik vilket skadar komponenter.

### 2.5.2 Ventilation

Ett it-utrymme ska alltid förses med lämplig nivå av luftomsättning och tillföras friskluft. Utrymmet bör därför förses med till- och frånluftsventilation. Tilluft bör förses med filter för att förhindra att smutsig luft kommer in i utrymmet. Mängden tillförd luft bör också skapa ett tydligt identifierbart övertryck i it-utrymmet, i förhållande till angränsande utrymmen. Genom övertrycket förhindras att damm och smuts ”sugs” in i it-utrymmet och skadar utrustning. Alla ventilationstrummor ska också förses med brandspjäll som är anslutna till fastighetens brandlarm och stänger av ventilationen till it-utrymmet i händelse av en brand. Finns det ett separat brandlarm i it-utrymmet kan brandspjäll med fördel även anslutas till detta larm som sannolikt upptäcker en brand tidigare än fastighetens larm.

*Bild 10. Brandspjäll anslutet till brandlarm monterat på en ventilationskanal.*

Eftersom ett it-utrymme klassas (i byggnormer och liknande regleringar) som ett tekniskt utrymme medför detta att man inte behöver tillföra friskluft i samma omfattning som för exempelvis ett kontor. Av denna anledning kan man ibland välja att endast installera tilluft, dvs. ventilationskanaler för frånluft eller överluft finns inte.

### 2.5.3 Luftcirkulation

Luftens cirkulation i ett it-utrymme är en vital aspekt för att it-utrustning ska kylas och värmen i utrymmet ska transporteras bort.

> Luftcirkulationen är en mycket viktig faktor för att skapa en ändamålsenlig miljö i it-utrymmet. Se alltid till att den kylda luften kan flöda fritt till den utrustning som ska kylas. Avlägsna alla hinder som kan störa luftcirkulationen.

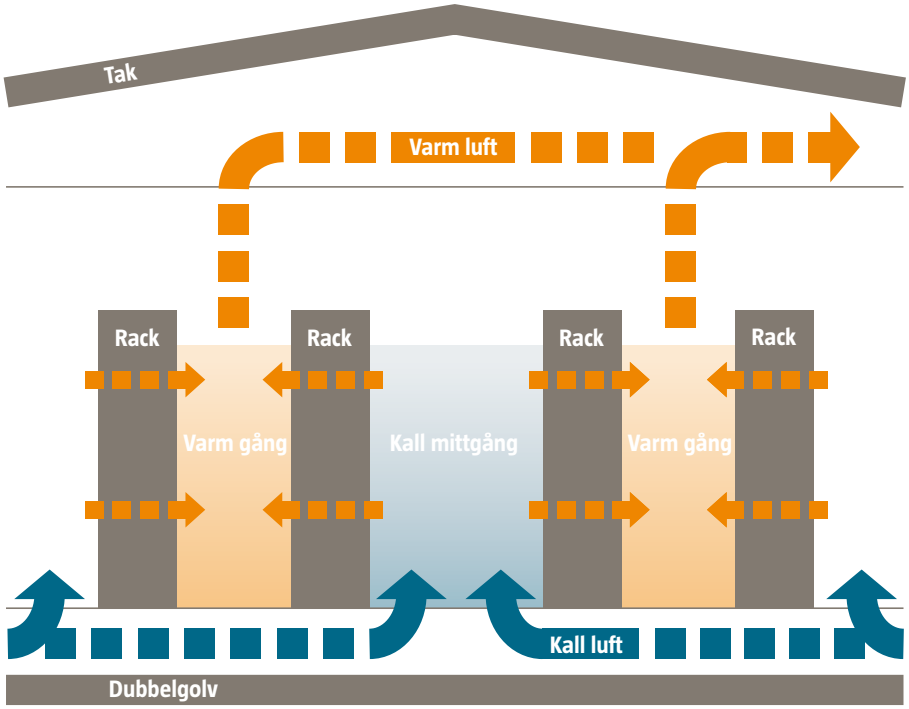
Flera varianter av luftcirkulation existerar hos verksamheter, som exempelvis:

- **Väggmonterad kyla**
  Luftcirkulationen har sitt ursprung i ett väggmonterat aggregat eller väggmonterad ventilationskanal. Förekommer vanligen i mindre it-utrymmen.
- **Takmonterad kyla**
  Luftcirkulationen har sitt ursprung i ett takmonterat aggregat eller takmonterad ventilationskanal. Förekommer vanligen i mindre till medelstora it-utrymmen.
- **Underblåsande kyla**
  Kyld luft transporteras under ett installationsgolv och släpps upp i eller framför ett stativ, rack eller hylla. Vanligast förekommande typen i medelstora till stora it-utrymmen av typ datorhallar.

*Bild 11 (till höger). Underblåsande kyla under installationsgolv, kyld luft passerar genom de perforerande plattorna.*

- **Rackmonterad kyla**
  Kylaggregat sitter monterade i (vanligen mellan) rack eller stativ. Relativt ovanligt, men förekommer i större it-utrymmen av typ datorhallar.
- **Överblåsande kyla**
  Kyld luft blåses ovanifrån stativ eller rack via utrustning monterad på stativets eller rackets tak. Relativt ovanligt, men förekommer i större it-utrymmen av typ datorhallar.

I små it-utrymmen, där mindre mängder it-utrustning finns, brukar typen av luftcirkulation inte spela någon större roll så länge tillräckligt med kyld luft tillförs. Bygger man däremot tätt mellan utrustning, koncentrerar montage i någon del, installerar utrustning som utvecklar värme mer koncentrerat, kommer man sannolikt att behöva kontrollera och åtgärda luftcirkulationen. I större it-utrymmen med stora mängder it-utrustning är luftcirkulationen viktigare för att tillräckligt med kyld luft ska nå all utrustning. I dessa utrymmen är den underblåsande typen av kyla vanligast (se bild nedan).




*Figur 3. It-utrymme med underblåsande kyla.*

I de flesta it-utrymmen används idag rack, stativ eller hyllor. It-utrustning suger in kyld luft på en sida och blåser ut uppvärmd luft på motsatt sida. Det råder i stort konsensus bland tillverkare av it-utrustning om denna kylfunktion. Som bilden ovan visar sugs den kylda luften in på ena sidan av stativet och uppvärmd luft blåses ut på motsatt sida. Detta skapar kalla och varma gångar mellan rack/stativraderna i it-utrymmet. Den uppvärmda luften stiger och cirkuleras tillbaka till kylaggregatet för att kylas på nytt. På detta sätt kan man hålla en konstant temperatur i utrymmet.

I bilden på sidan 43 används underblåsande kyla som transporteras under ett installationsgolv. Galler i installationsgolvet placeras på den sida av stativet/racket där utrustningen suger in luft. På motstående sida monteras inga galler i installationsgolvet.

Det är viktigt att den uppvärmda luften kan transporteras bort i tillräcklig omfattning samt att man har ett tillräckligt tryck under installationsgolvet i kombination med ett väl justerat luftflöde. Om detta inte sker kan den uppvärmda luften ”ramla ned” på den kalla sidan igen och it-utrustningar högt uppe i stativ/rack använder då denna varma luft som sin kylda luft. Om man har problem med att it-utrustningar högt upp i stativ/rack löpande slutar att fungera, har man sannolikt detta problem.

> Tänk på hur it-utrustning monteras i rack, stativ eller hylla. Det är fortfarande vanligt att utrustning vänds åt fel håll och att varm luft därför sugs in istället för kyld luft. Detta kan skada utrustningen.

### 2.5.4 Kylanläggningens typ

Det finns flera olika typer av kylanläggningar på marknaden. Och det är viktigt att man använder en typ av kylaggregat som är anpassat till it-miljöer och till det utrymme som man avser att kyla. Vanliga typer av kylaggregat och -begrepp inkluderar:

- **Komfortkyla**
  Används normalt i bostadshus och kontor för att kyla inomhusluften under enskilda varma dagar. Denna typ är normalt inte avsedd för kontinuerlig drift. Typen klarar av jämn temperatur, men saknar oftast möjligheter att befukta och avfukta luft.
- **Industri- och processkyla**
  Centralt installerad anläggning som normalt används för att kyla industrilokaler, affärer eller exempelvis ishallar. Normalt anpassad för kontinuerlig drift men ofta sämre på att hålla jämn temperatur, saknar oftast möjligheter att befukta och avfukta luft.
- **Precisionskyla**
  Typ anpassad för kylning av elektrisk utrustning där kyleffekten koncentreras till specifika platser (punkter) i ett utrymme. Typen är anpassad till kontinuerlig drift och har möjlighet att hålla jämn temperatur och konstant relativ luftfuktighet.
- **Reservkyla**
  Om ordinarie kylaggregat slutar att fungera måste en annan funktion ta över. Reservkyla utgörs normalt av ytterligare ett kylaggregat. Mer vanligt är dock att två aggregat körs kontinuerligt med max 50 % belastning. Slutar ett att fungera finns kapacitet över för att kyla utrymmet med ett aggregat. Denna lösning kallas också för dubbla eller redundanta kylaggregat.
- **Nödkyla**
  Nödkyla kan kopplas till de flesta typer av kylaggregat. Principen bakom nödkyla bygger på att man tillför ytterligare en köldbärare till kylaggregatet. Vanligaste typen av köldbärare är vanligt dricksvatten (även kallat stadsvatten). Om fel upp-

träder i den ordinarie (primära) köldbäraren kopplas nödkylan in. Observera att nödkyla inte skyddar mot fel i själva aggregatet som exempelvis ett elektriskt fel. Funktionen nödkyla ska testas regelbundet av kompetent personal.

- **Frikyla**
  Principen bakom frikyla är att utnyttja en extern miljö för att nå en lägre effektförbrukning. Den externa miljön kan exempelvis vara utomhusluft eller ett närliggande vattendrag. Istället för att kyla vätskan i köldbärare med kylanläggningens komponenter (kompressor), vilket är relativt kostnadskrävande, låter man kall utomhusluft eller kallt sjövatten göra samma sak. Anpassning till frikyla gör lösningen kostnadseffektiv och miljöriktig.
- **Fjärrkyla**
  I större städer kan kyla också finnas att köpa via en anslutning till en fjärrmatad köldbärare (samma princip som fjärrvärme). Denna typ av kyla är dock mest anpassad till kontors- och affärslokaler och lämpar sig mindre bra för it-utrymmen, speciellt om dessa är kritiska. Använd aldrig fjärrkyla i it-utrymmen utan nödkyla. Leverantörer av fjärrkyla ser normalt inte sin leverans som kritisk och kan därför göra oanmält underhåll och service som stör leveranser.

***Bild 12.*** *Frikyla placerad utomhus för att nyttja utomhusluft.*

Klimatanläggningar av typen komfortkyla är inte lämpliga att använda i it-utrymmen, eftersom dessa normalt inte är anpassade för kontinuerlig drift.

Vilken typ av kyla man bör välja beror på (som ses ovan) vilka förutsättningar den enskilda verksamheten har rent geografiskt samt hur lokalerna i fastigheten är planerade och utrustade. Storleken (golvyta och takhöjd) hos it-utrymmet samt mängden av it-utrustning som man avser att kyla är vanligtvis också en avgörande faktor.


***Bild 13.*** *Display på en anläggning av typen precisionskyla.*

Konsultera alltid expertis inom kyla och miljö för anpassningar i it-utrymmen. Använd expertis som har erfarenhet av kylinstallationer i it-miljöer.

**Grön kyla**

Begreppet grön kyla börjar användas mer och mer. Detta innebär egentligen att man tar tillvara den värme som alstras i it-utrymmet och återvinner den. Värmen används vanligtvis för att värma övriga lokaler och utrymmen i den fastighet som it-utrymmet befinner sig i. Grön kyla är således kostnadseffektivt och miljöriktigt.

Hos många företag och organisationer har man en alltför låg temperatur i sina it-utrymmen. Temperaturer omkring 18–19 grader Celsius är relativt vanligt. Lufttemperaturen kan många gånger höjas till 22–24 grader Celsius utan att detta påverkar it-utrustningen i utrymmet negativt. En höjning med 3–5 grader motsvarar en avsevärd kostnadsbesparing och minskar också miljöpåverkan. Vid en informationssäkerhetsanalys rekommenderades en verksamhet i östra Sverige att höja temperaturen med 4 grader i sina två datorhallar. Beräkningar visade en besparing på ca 300 000 kronor per år i minskade energikostnader.

### 2.5.5 Kylkapacitet

En aspekt som diskuteras flitigt vid installationer av kyla är kapacitet, d.v.s. den kyleffekt som kylaggregatet ska leverera. Förenklat ska kyleffekten dimensioneras så att den värme som tillförs luften från it-utrustningen kan tas om hand och åter kylas ned. Temperaturen ska hållas konstant inom rekommenderade värden.

Ett fullhöjdsrack där it-utrustning har monterats efter tillverkarens rekommendationer utvecklar normalt mellan 2 och 4 kilowatt värmeeffekt. Men det finns exempel, där vissa typer av it-utrustning används och där montagen är täta, där värmeeffekter på 30–40 kilowatt per rack har uppmätts. För de flesta verksamheter brukar man dock kunna använda övre gränsen om 4 kilowatt gånger antal stativ/rack för att få en uppfattning om kyleffektsbehovet.

Ytterligare ett sätt för att få fram kyleffektsbehovet är att beräkna utifrån märkeffekten på alla it-utrustningar i utrymmet. Detta kan vara tidsödande och tenderar också att ge en något felaktig bild över behovet eftersom inga it-utrustningar förbrukar märkeffekten hela tiden.

Det finns mer avancerade former av beräkning för kyleffekter som används av expertis inom området. I bilaga 4 finns en förenklad beräkningsmodell för att uppskatta kyleffektsbehov men konsultera alltid expertis för en mer detaljerad och korrekt beräkning.

### 2.5.6 Relativ luftfuktighet

It-utrustning och datamedia är i allmänhet känsliga för om den relativa luftfuktigheten varierar alltför mycket. Det optimala värdet för den relativa luftfuktigheten i ett it-utrymme är kring 50 %, men variationer mellan 30 och 70 % brukar anses som godtagbart. Om värdet sjunker under 30 % finns det risk att statisk elektricitet kan bildas i utrymmet och i utrustningen. Ökar värdet över 70 % finns det istället risk att vätska fälls ut ur luften och skadar utrustning och datamedia. Tänk på att värdet för relativ luftfuktighet i en byggnad är relaterat till utomhusluften (om teknisk reglering av relativ luftfuktighet saknas). Vilket leder till stora fluktuationer mellan olika årstider.

> I slutet av 1990-talet hade en verksamhet i norra Sverige problem med att servrar och kommunikationsutrustning i en datorhall av oförklarliga skäl havererade. Antalet haverier ökade under vinterhalvåret. Vid en analys av den fysiska informationssäkerheten i fastigheten konstaterades att den relativa luftfuktigheten var mycket låg i det aktuella utrymmet. Mätvärden mellan 13 och 15 % identifierades. Verksamheten skaffade utrustning för att befukta luften och problemen försvann.

### 2.5.7 Damm och smuts

De flesta typer av it-utrustning innehåller fläktar för att kyla elektronik. Eftersom luft normalt alltid passerar genom it-utrustningar är det viktigt att luften är ren. Alla former av inkommande luft (tilluft) till ett it-utrymme bör vara fria från damm och smuts. Alla ytor inne i ett it-utrymme bör rengöras löpande. Damm som samlas i tekniska utrustningar i ett it-utrymme kan agera katalysator vid exempelvis en kortslutning och starta ett brandförlopp. (Se även avsnitt 2.5.2)

## 2.6 El och datanät

Större strömavbrott är relativt ovanliga i Sverige om man jämför med andra länder. Avbrott i själva elkraftförsörjningen till en fastighet förekommer sällan. Vanligare är däremot strömavbrott inne i fastigheter och lokaler som är förorsakade av mänskliga faktorer eller andra lokalt begränsade fenomen. Oavsett vad som orsakar strömavbrotten får dessa inte påverka it-utrustningar och tillgängligheten till information i it-system. Riskerna för att störningar i elmatning påverkar it-drift reduceras genom att anpassa installationer och införa lämpliga skydd.

### 2.6.1 Installation

All elektricitet i ett it-utrymme ska alltid planeras, projekteras och installeras av behöriga utförare. Även om externa parter utför själva installationen bör en beställare övergripande känna till de aspekter och begrepp som är speciella för el i ett it-utrymme[16].

***Bild 14.*** *Ställverk som matar it-utrymme placerade i separat utrymme skilt från it-utrustning.*

I ett it-utrymme har elkraft ofta ett beroende som kräver speciella anpassningar. Undvik därför att använda företag eller organisationer som inte har vana att arbeta med el i it-miljöer, även om dessa har formell behörighet.

Nedan följer några omständigheter som medför krav på anpassningar för el i ett it-utrymme samt rekommendationer för hur anpassning ska göras:

16. Enligt Riksarkivets föreskrifter ska arkivlokalens belysning utgöras av lysrörsarmatur som har ett tillfredsställande skydd mot damm. Lysrörsarmaturen ska vara försedd med säkerhetsglimtändare eller högfrekvensdon. Myndigheten/organisationen bör välja armatur i kapslingsklass lägst IP 43 enligt standard för Kapslingsklasser för elektrisk materiel SS-EN 60529 utgåva 1 (RA-FS 2013:4, 7 kap. 10 §).

- **Huvudmatning**
  Den huvudsakliga matningen av elkraft till ett it-utrymme ska alltid vara skild från fastighetens övriga allmänkraft och belysning. It-utrymmen bör därför förses med separat trefasmatning och egna elcentraler.
- **Dubblerad huvudmatning**
  I särskilda fall kan det finnas behov av dubbla huvudmatningar från separerade lokalnät med matning från olika elkraftsleverantörer.
- **Flera typer av elkraft**
  Ett it-utrymme designas vanligen med två eller tre typer av elkraft. Typen av elkraft klassificeras normalt utifrån robusthet, dvs. hur motståndskraftig strömkällan är mot störningar. Högst i skalan ligger normalt primärkraft (avbrottsfri kraft – ofta kallad A-kraft). Därefter följer typen sekundärkraft (ofta kallad B-kraft). B-kraft kan också vara avbrottsfri om man använder flera uppsättningar utrustning för avbrottsfri kraft. B-kraft saknar dock vanligen denna egenskap och utgörs normalt av allmänkraft. Är sekundärkraften avbrottsfri finns vanligen också allmänkraft i it-utrymmet för exempelvis belysning och tillfälliga anslutningar av elektrisk utrustning och maskiner.


***Bild 15.*** *A- och B-kraft med fast montage i stativ. I detta fall används DC (likström) och det börjar förekomma fler servrar som matas med enbart DC istället för AC/DC på grund av energieffektivitet. Samma princip med A och B kraft gäller för både DC och AC/DC.*

- **Kanalisation**
  Installationen av el bör ske på egna kabelstegar och skiljas från övriga kablar i it-utrymmet. Se alltid till att ha kapacitet för utbyggnad av el i kanalisationen. Var noggrann med att inte installera kabelstegar så att de stör luftflödet eller luftcirkulationen i utrymmet. Ett vanligt misstag är att kabelstegar under installationsgolv monteras tvärs luftflödet under golvet och stör kylan till utrustningen.

- **Allmänbelysning**
  Anpassad belysning (med exempelvis HF-don) för tekniska utrymmen ska användas. Belysningen ska inte vara ansluten till samma elcentral som it-utrustningen i hallen. Lysrörsarmaturer som innehåller glimtändare ska undvikas eftersom de kan utgöra en brandfara.
- **Säkerhetsbelysning**
  It-utrymmen ska vara utrustade med säkerhetsbelysning som aktiveras vid strömavbrott och visar vägen vid evakuering.
- **Serviceuttag**
  Det ska alltid finnas minst ett uttag som är tydligt märkt i ett it-utrymme som är skilt från it-utrymmets egna elcentraler. Dessa uttag brukar benämnas service-uttag och ska användas för att ansluta elektriska apparater vid arbeten i utrymmet, som exempelvis dammsugare, borrmaskiner eller annan liknande utrustning.
- **Fördelning av matning, matning till stativ**
  Mata varje stativ eller rack med minst två separata grupper, A- och B-kraft i förekommande fall.
- **Fördelare i stativ**
  Använd alltid fast monterade fördelare i hyllor, rack och stativ. Använd aldrig fördelare som har strömbrytare monterade på fördelare eller kabel.
- **Avsäkrad utrustning**
  Man bör försöka att avsäkra all utrustning i utrymmet separat. Åtminstone ska man gruppera utrustning på ett sådant sätt att en enskild utlöst säkring inte får följdeffekter på annan utrustning. Det finns en typ av elfördelare som brukar benämnas PDU[17]. En PDU är normalt anpassad för rack-montage. Dessa enheter, beroende på typ, kan ha möjligheter till separat avsäkring, mätning av effekt och förbrukning eller andra typer av fjärrstyrning.

Försök alltid separera beroendet mellan it-utrustningar i deras elanslutningar och se till att it-utrymmet har förutsättningar för att göra denna separation. Gruppera exempelvis aldrig utrustningar som har samma funktion (exempelvis ett redundant it-system) i samma fördelare, grupp eller fas.

- **Märkning**
  Märk alla uttag (både för el och data) i ett it-utrymme noggrant. Använd helst olika färgkombinationer för att kunna skilja på olika typer av elmatning, såsom allmänkraft, primär- och sekundärkraft, avbrottsfri kraft, reservkraft osv.
- **Anslutning av it-utrustning**
  Koppla alltid in it-utrustning som har redundant elförsörjning i en separat grupp-säkring. Anslut aldrig it-utrustning som är redundant i samma gruppsäkring.

Det är mycket vanligt att leverantörer av it-utrustning ansluter dubbla kraftaggregat i samma säkringsgrupp. Beställaren bör säkerställa att detta inte sker.

17. Power Distribution Unit – Fördelare för elkraft


NÖDLJUSFUNKTION ENDAST
MED STRÖMSTÄLLARNA
INSTÄLLDA På HUVUDLJUS
ELLER LEDLJUS

En processindustri i södra Sverige var ansvarig för hela koncernens datatrafik och gemensamma it-system. Man fungerade därför som kommunikationsnav för alla övriga verksamheter. Vid ett strömavbrott i datorhallen slogs hela koncernens datatrafik ut och åtkomsten till gemensamma system. Felorsaken lokaliserades till en utlöst automatsäkring. Vid närmare analys konstaterades att alla kommunikationsutrustningar var placerade i samma gruppsäkring. Hade man separerat kommunikationsutrustningarna hade omfattningen av störningen minskat avsevärt.

- **Kritisk it-utrustning med enskilt kraftaggregat**
  Många it-utrymmen har kritisk it-utrustning som saknar dubbla kraftaggregat. Använd elektriska switchar som ansluts till två separata grupper med en utgång till dessa utrustningar.
- **Apparatkablage**
  Använd olika färger på apparatkablage för att kunna skilja på primär och sekundär kraftmatning.

### 2.6.2 Reservkraft

Reservkraftförsörjning (även kallat reservkraft, reservel eller backupkraft) är ett system för att skapa elektricitet oberoende av det allmänna elnätet när normal strömförsörjning faller bort. Detta är önskvärt på många ställen där man bedriver viktig verksamhet som inte får påverkas av strömavbrott, till exempel sjukhus, flygplatser, kraftverk eller it-utrymmen.

Förväxla inte reservkraft med avbrottsfri kraft. Detta är två olika typer av anläggningar som har helt skilda uppgifter när ett strömavbrott inträffar.

En anläggning för reservkraft består normalt av en motor, en generator och ett styrsystem. Den vanligaste typen av anläggning är dieseldriven men det finns också bensin- och gasdrivna anläggningar. När ett strömavbrott sker kommer styrsystemet att reagera och initiera uppstart av anläggningen, ett batterisystem behövs därför för att kunna förse anläggningen med el under uppstart.

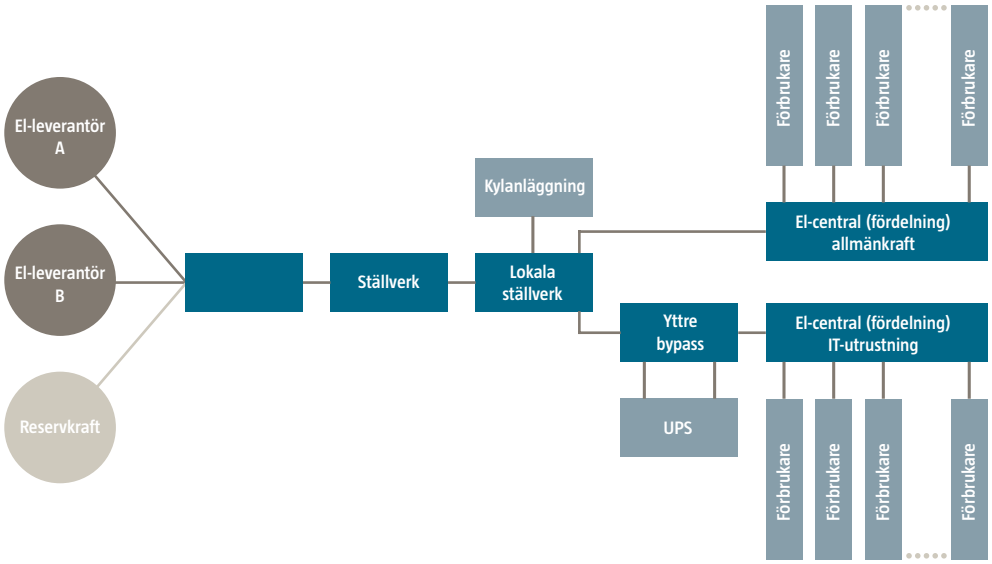
Reservkraftverkets styrning kan antingen vara helt automatisk, delvis automatiserad eller manuell. Normalt sker uppstart helt automatiskt vid ett upptäckt avbrott. Återgång till normal matning görs manuellt, på en manuell till-order eller helt automatiskt beroende på typ av system.

För att en reservkraftanläggning ska kunna leverera ström så måste det som ska strömförsörjas avskiljas från det övriga elnätet, dessutom måste någon form av aktiv laststyrning finnas på större anläggningar. Normalt sett löser man detta genom att starta anläggningen med enbart de viktigaste elförbrukarna inkopplade och därefter successivt lägga på mer last tills man är i full drift.

***Bild 16 (till vänster).*** *Batterimatad säkerhetsbelysning.*

Under en skarp uppstart kan det som ska strömförsörjas vara spänningslöst varpå ingen fasning behövs. Men i ett it-utrymme är vanligen utrustningen strömförsörjd av avbrottsfri kraft och automatisk synkronisering måste finnas inbyggd för att ge möjlighet till blinkfri övergång. Detta kan vara beroende på vilken typ av avbrottsfri kraft som används. För att förhindra att själva reservkraftanläggningen, eller det den är kopplad till, skadas så finns ett flertal säkerhetssystem som hela tiden övervakar anläggningen.

Ur it-utrymmets perspektiv ansluts anläggningen för reservkraft parallellt med inkommande nätanslutning (elnätet) och seriellt i förhållande till den avbrottsfria kraften (UPS). Se principskiss nedan.




***Figur 4.*** *Principskiss över elförsörjning inklusive reservkraft och UPS.*

***Bild 17.*** *Reservkraft dieselaggregat placerat utomhus. Placering av tank förenklar påfyllning av bränsle.*

Som nämns i kapitel 2.6.6 är det en UPS-enhets uppgift att försörja it-utrustningen med elkraft tills det att reservkraften är fullt uppstartad. Normalt tar denna procedur 20–30 sekunder. När reservkraften är fullt uppstartad och infasad kommer de enheter i it-utrymmen som inte har varit försörjda av avbrottsfri kraft att kopplas in och normal drift återställs. Normalt benämner man denna status som reservdrift, reservläge eller motsvarande.

Hos mindre verksamheter är det vanligt att man skaffar reservkraft enbart för att kunna förse utrustningen i sina it-utrymmen med elkraft. Övriga delar i fastigheten blir strömlösa vid ett avbrott. Större verksamheter kan ha reservkraftanläggningar som försörjer hela fastigheter eller områden. När det sker förändringar i våra it-utrymmen är det viktigt att man inte glömmer bort att kontrollera att den effekt som anläggningen för reservkraft kan leverera inte överskrids. Förbrukningen hos modernare it-utrustning ökar generellt.

### 2.6.3 Bränsle för reservkraft

När en reservkraftanläggning har startats upp vid ett strömavbrott kommer anläggningen att mata elkraft till alla it-utrymmen tills det att anläggningens bränsle tar slut. Beroende på vilken typ av verksamhet som bedrivs har man vanligen bränsle för längre reservdrift om verksamheten är kritisk eller exempelvis samhällsviktig, vanligen 5–7 dagar. En riskanalys bör genomföras tillsammans med verksamhetsansvariga för att fastställa hur länge reservdrift minst ska kunna pågå utan avbrott.

Efter strömavbrottet i Kista år 2001 valde många verksamheter som enbart hade haft tillgång till avbrottsfri kraft (UPS) att skaffa anläggningar för reservkraft eftersom avbrottet varade en längre tid. Liknande negativ påverkan skulle nu kunna undvikas i framtiden. När ett liknande längre strömavbrott inträffade ett år senare fick många verksamheter bränslebrist och försökte förgäves kontakta leverantörer för påfyllning. Dessa leverantörer var dock redan fullt sysselsatta med att fylla på bränsle hos de verksamheter som hade varit kloka nog att teckna serviceavtal som inkluderade detta moment. Hos många verksamheter uppstod därför samma strömlösa situation som året innan trots att man hade vidtagit åtgärder.

Det vanligaste bränslet i våra anläggningar för reservkraft är idag diesel. Diesel som bränsle åldras och behöver bytas ut med löpande intervall. Det kan annars finnas en risk för att reservkraftanläggningen inte startar vid ett skarpt läge. Det finns varianter av diesel på marknaden som är mer lagrings-/åldersbeständigt och inte behöver bytas ut lika ofta. Lagringsbeständigheten kan vara 5 eller 10 år. Kontrollera med er leverantör av bränsle.

Använd inte miljöbränsle eftersom detta innehåller komponenter från växtriket som möglar och ”växer”. Det finns motortillverkare som inte lämnar några garantier om man använder miljöbränsle.

### 2.6.4 Underhåll och service

Alla typer av reservkraftanläggningar är i behov av löpande service och underhåll. En verksamhet bör alltid även ha egna rutiner för att med jämna mellanrum kontrollera reservkraftens funktion. Har den egna verksamheten inte kompetens för drift och underhåll av en reservkraftanläggning bör man etablera en relation med en extern part som ansvarar för all service och underhåll. Underhåll, kontroll och service av batterier är mycket viktigt. Det finns exempel där verksamheter har slarvat med denna aktivitet vilket har resulterat i att skyddet inte har fungerat vid skarpa situationer.

### 2.6.5 Mobil reservkraft

En annan typ av reservkraft som finns på marknaden är mobil reservkraft. Denna lösning är baserad på att en extern avtalspart levererar en mobil anläggning i händelse av strömavbrott. Vanligen sker denna leverans genom att en lastbil med en kraftanläggning på flaket ansluter en kabel till fastigheten på en förutbestämd överlämningspunkt. Mobil reservkraft är relativt ovanligt i Sverige.

### 2.6.6 Avbrottsfri kraft

Avbrottsfri kraftförsörjning (UPS, Uninterruptible Power Supply) är en teknisk utrustning som tillhandahåller en hög kvalité på lik- eller växelspänning till elförbrukare, även om ett strömavbrott eller andra störningar uppstår. En UPS installeras mellan den ingående kraftmatningen och elförbrukaren (it-utrustningen).

Beroende på vilken typ av UPS som används är det möjligt att skydda ansluten utrustning mot flera olika typer av störningar såsom avbrott, under- och överspänning samt störningar i kvalitén hos spänningen såsom frekvensstörningar och övertoner. De vanligaste typerna av UPS är:

- **Off-line (standby)**
  Skyddar mot avbrott samt korta under- och överspänningar. Enheten kopplas endast in vid ett avbrott, under normal drift levereras spänning till elförbrukare från elnätet(allmänkraft). Typen är lämplig att använda i mindre installationer eller mindre kritiska verksamheter.
- **Line interactive (power boost)**
  Skyddar mot avbrott, under- och överspänningar samt vissa störningar i kvalité. Funktionen vid avbrott är lika som för typen off-line. En line interactive UPS är också försedd med logik som övervakar kvalité som inkommande matning och kan vidta vissa kompenserande åtgärder. Denna typ av UPS kan användas i mer kritiska installationer, men används normalt i mindre till medelstora installationer.
- **On-line**
  Skyddar mot avbrott, under- och överspänningar samt alla störningar i kvalité. Den största skillnaden mot de två andra typerna är att elkraften från inkommande matning inte används i utgående matning, matningen sker alltid från UPS-enheten (därav benämningen on-line). Denna typ kallas också för dubbelkonverterande UPS eftersom inkommande växelspänning först konverteras till likspänning, följt av en återkonvertering till växelspänning på utgången. På detta sätt levereras alltid en störningsfri matning till elförbrukare. Denna typ av UPS används vanligen i större eller kritiska installationer.

***Bild 18 (till höger).*** *Anläggning för avbrottsfri kraft (UPS) med tillhörande batterier placerade i stativ.*


EMERSON
200kVA

### 2.6.7 Enfas och trefas UPS

Mindre UPS-enheter (vanligen under 5 kVA[18]) är normalt av typen enfas. UPS-enheten placeras normalt inne i rack/stativ eller i direkt närhet till den utrustning den ska försörja. En enfas UPS placeras normalt efter elcentralen i it-utrymmet vilket medför att om den gruppsäkring UPS-enheten är ansluten till löser ut, så kopplas UPS-enheten in. När batteriet tar slut slutar enheten att leverera ström. Observera att ovanstående situation sker även om reservkraft är inkopplad och aktiv.

Större UPS-enheter (vanligen över 5 kVA) är oftast av trefas-typ. En trefas UPS ansluts alltid innan it-utrymmets elcentral och försörjer alla it-utrustningar som är anslutna till samma elcentral. Detta betyder att om en enskild gruppsäkring löser ut så kommer all utrustning ansluten till densamma att bli strömlös. Det är bl.a. av denna anledning det är så viktigt att avskilt säkra av utrustningar med mindre (lägre amperetal) säkringar.

I båda fallen med enfas och trefas UPS kan och bör man använda A- respektive B-kraft samt ha dubbla kraftaggregat för kritiska it-utrustningar. Ovanstående situationer där utrustningar blir strömlösa kan då undvikas.

### 2.6.8 Inre och yttre bypass

En UPS-enhet kan behöva bytas ut eller repareras. För att man ska minimera störningar på it-driften behövs ett sätt att koppla bort en UPS-enhet från elnätet. För detta behov finns två typer av mekanismer som kallas inre respektive yttre bypass. En yttre bypass medger att UPS-enheten kan kopplas bort helt från elnätet. En inre bypass kräver att enheten fortfarande är ansluten till elnätet men all elmatning till utrustning från UPS-enheten är inaktiverad och sker direkt från inkommande elmatning.

För vissa enfas UPS där man direktansluter it-utrustning finns inga lösningar där man kan koppla ur UPS-enheten med befintlig drift om man inte har tillgång till B-kraft. It-utrustningen måste helt enkelt stängas av under tiden eller startas om efter att man har valt en annan strömmatning. Det finns dock enfas UPS-enheter som har möjligheter till yttre bypass och därmed medger utbyte eller reparation utan driftsbortfall. En trefas UPS är normalt alltid utrustad med en bypass-funktion. Både en inre bypass- och en yttre bypass-funktion brukar finnas för en blinkfri övergång till matning från elnätet.

### 2.6.9 Central eller distribuerad UPS-lösning

En installation av en UPS kan göras på två sätt: antingen som en central lösning som matar alla elförbrukare i it-utrymmet via en central fördelning (elcentral) eller som en distribuerad lösning där enskilda UPS-enheter placeras ut i hyllor, skåp och rack och matar elförbrukare direkt. En central lösning är vanligare i större och mer kritiska installationer, medan distribuerade lösningar är mer vanligt hos mindre verksamheter utan höga tillgänglighetskrav. Centrala lösningar avvänder oftast on-line-typ av UPS, medan off-line- och line interactive-typerna är vanligare i distribuerade lösningar.

18. Se kapitel 2.6.10 för mer information gällande effekter.

Om man har behov för mer än 20 kVA avbrottsfri kraft i ett it-utrymme, kommer det att löna sig att välja en central UPS-lösning.

Båda lösningarna har sina respektive fördelar och nackdelar och dessa är viktiga att förstå vid val av lösning så att detta kan överföras till verksamhetens krav. Det är också möjligt att kombinera de två olika lösningarna med varandra.

**För- och nackdelar med central lösning**

| FÖRDELAR | NACKDELAR |
|---|---|
| Längre livslängd | Komplex installation |
| Bättre skalbarhet | Högre relativ kostnad |
| Enklare att övervaka och underhålla | En SPOF[19] införs |
| Lägre elförbrukning | Kräver större utrymme |
| | Behov av extern serviceorganisation |

**För- och nackdelar med distribuerad lösning**

| FÖRDELAR | NACKDELAR |
|---|---|
| Lägre relativ kostnad | Bristande skalbarhet |
| Enkel installation | Komplext underhåll och övervakning |
| Ingen SPOF | Svårt med omedelbar komplett nedstängning (nödstopp) |
| Anpassning till olika kravnivåer | |

### 2.6.10 UPS kapacitet och belastning

Kapaciteten hos en UPS, dvs. förmågan att leverera elkraft till utrustning i ett it-utrymme, mäts i enheten Volt Ampere (VA). Utrustningen i it-utrymmen och elförbrukares effekt mäts i Watt (W). Märkningen på it-utrustning representerar vanligen det interna kraftaggregatets maximala effekt som kan levereras till elektroniken inne i enheten.

Verksamheter dimensionerar ofta sin UPS-kapacitet fel eftersom man inte förstår de underliggande sambanden mellan Volt Ampere(VA) och Watt(W) samt hur utrustningen i it-utrymmet förbrukar energi.

19. Single point of failure (SPOF). Enstaka punkt i ett system i vilken ett uppträdande fel leder till omfattande funktionsförlust.

Konsultera alltid expertis för hjälp med att beräkna en korrekt dimensionering av en UPS. I bilaga 5 finns en övergripande beräkning av dimensioneringen.

Tänk på att it-utrustning alltid förbrukar mer effekt vid uppstart. Om man ligger nära sin maximala UPS-kapacitet, kan det vara möjligt att bedriva normal it-drift. Men när utrustningen ska startas om efter ett oplanerat strömavbrott eller efter ett rutinmässigt underhållsarbete klarar man inte av att starta utrustningen eftersom man överbelastar UPS-enheten. Detta resulterar ofta i att man tvingas att starta utrustning i sekventiell ordning, en och en efter varandra. Har man stora mängder utrustning kan detta ta mycket lång tid. Om bypass finns minskar man normalt risken för att denna situation uppstår.

En trefas UPS ska aldrig ”snedbelastas”, dvs. respektive belastning på de tre faserna ska i möjligaste mån vara lika. UPS-enheten kan ta skada om man fördelar ojämnt. Kontrollera UPS-enhetens display med jämna mellanrum och flytta it-utrustning till andra grupper som matas av en annan fas om denna situation uppstår.

### 2.6.11 UPS-batterier

För att en UPS ska kunna leverera elkraft efter ett avbrott måste den utrustas med en batterifunktion. Det är batteriernas uppgift att leverera el till it-utrustningen tills nätspänning kan återställas från elnätet eller från reservkraft.

Tänk på att inte förväxla begreppen för en UPS batterikapacitet och en UPS förmåga att leverera tillräcklig omfattning av elkraft, dvs. effekten. Tänk också på att inte överdimensionera batteritiden hos UPS-enheterna.

Batterierna i en UPS ska dimensioneras så att de klarar att leverera den effekt som krävs. Eftersom likström från batterierna konverteras till växelström av UPS-enheten krävs relativt få batterier. Men för att batterierna inte ska laddas ur omedelbart krävs att storleken på batterierna utökas eller, förenklat, att antalet batterier utökas. Dimensioneringen av batterierna i en UPS är alltså framförallt en fråga om **hur länge** batterierna klarar av att leverera el till UPS-elektroniken innan de laddas ur. Det är batteritiden som kapacitetsfaktor som är mest intressant.

Batteritiden hos en UPS ska maximalt dimensioneras till 15–20 minuter. Batteritiden ska heller aldrig underdimensioneras och en UPS-enhet bör minst klara 8–10 minuter utan ordinarie kraftmatning. Orsaken till dessa relativt snäva marginaler är den värmeutveckling som it-utrustningar ger ifrån sig. Kylaggregaten i ett it-utrymme är normalt aldrig anslutna till avbrottsfri kraft och kommer

därför omedelbart att upphöra att fungera vid ett strömavbrott. Utan kyla stiger temperaturen i ett it-utrymme snabbt (som tidigare har beskrivits) och därför måste batterierna hinna laddas ur för att värme inte ska skada it-utrustning och datamedia.

De flesta UPS-enheter har funktioner för att övervaka ovanstående händelseförlopp och är försedda med mekanismer för att skicka manöverkommandon till it-utrustningar. Om kraftmatning inte återställs inom en viss tid kan UPS-enhetens logik initiera automatisk avstängning av it-utrustning och förhindra värmeökning.

Om en verksamhet har tillgång till reservkraft är situationen annorlunda. Kylaggregaten kommer då inte att stängas ner (förutom under den tid det tar att starta upp reservkraften) och miljön i utrymmet är då fortfarande kontrollerad. Finns reservkraft att tillgå är därför detta ett motiv till att **minska kraven på batteritid ytterligare**. Dock ska man alltid ta hänsyn till situationen om reservkraften inte startar upp som avsett, då kan lite extra batteritid ge personalen möjligheter att manuellt genomföra en kontrollerad nedstängning av utrustningen innan temperaturen har ökat för mycket.

### 2.6.12 Datakablage – datanät

All dragning av datanät och datakablage i ett it-utrymme är av typen svagström och ska skiljas från andra elinstallationer. Detta gäller även fiberkablar. Datakablage ska läggas på egna kabelstegar väl avskilt från starkströmskablar för att undvika att störningar sker.

Vissa typer av verksamheter kan också ha krav på att dragningen av kablar ska skyddas från åverkan och manipulering. Hos andra typer av verksamheter som hanterar extremt känslig information kan det finnas krav på att allt datakablage är draget på ett sådant sätt att inspektion underlättas. Var kablage är draget är avgörande för vilken typ av skydd som krävs eller om kablaget ska dras öppet.

## 2.7 Vätska

Elektronisk utrustning och datamedia är känsliga för vätska. Större läckage där stora mängder vätska tränger in i ett it-utrymme kan vara förödande men även mindre läckage kan allvarligt skada utrustning och datamedia.

### 2.7.1 Vätska utanför it-utrymmen

Installationer av vätskebärande rör är generellt vanligt förekommande där it-utrymmen är placerade. Avloppsrör, värmebärare och köldbärare i rör med relativt grov diameter finns ofta i direkt närhet. Trycksatta rör utgör vanligen de största hoten eftersom läckage kan medföra att stora mängder vätska läcker ut. Icke trycksatta rör (t.ex. avloppsrör) läcker normalt inte samma volym vätska per tidsenhet och utgör därför inte ett lika stort hot.

Många it-utrymmen är placerade (se kapitel 2.1 om placering) i källarplanet i fastigheter vilket gör dem extra känsliga för vätskeläckage eftersom vätskan inte har någonstans att ta vägen. Om ett it-utrymme är placerat ovan mark och ett läckage sker, finns det nästan alltid en naturlig evakuering av vätska ner i schakt, trappor eller utgångar. Riskerna för direkt påverkan på it-utrymmet minskar då, men indirekta risker kan fortfarande existera om läckaget sker till källarutrymmen som exempelvis matar it-utrymmen med el.

Kartlägg alltid alla risker för läckage av vätska från rördragningar utanför ett it-utrymme.

### 2.7.2 Vätska inne i it-utrymmen

De flesta it-utrymmen innehåller vätskeinstallationer i någon form. Köldbärare till kylanläggningar finns ofta i it-utrymmen och denna rördragning är egentligen den enda typ som bör tillåtas i it-utrymmen. Tyvärr är det vanligt att it-utrymmen innehåller även andra typer av rördragningar som värmerör, färskvattenrör och avloppsrör. En vanlig situation är att verksamheten har blivit tilldelade utrymmet och inte haft möjlighet att undvika riskerna med olämpliga rördragningar. Tyvärr är det också vanligt att brunnar för evakuering av vätska saknas[20].

Var noggrann med att inga rördragningar inne i ett it-utrymme passerar ovanför it-utrustning och datamedia.

### 2.7.3 Vätskeskydd

Finns det uppenbara risker för vätskeläckage ska man vidta åtgärder för att minska dessa risker. Själva installationerna bör om möjligt omlokaliseras. Saknas dessa möjligheter ska man införa skydd. Nedan följer ett antal förslag till förändringar och riskminimerande åtgärder som kan övervägas:

- **Omlokalisering**
  Se över möjligheterna att omlokalisera riskfyllda rördragningar. Försök att begränsa rördragningar i it-utrymmen till de som verkligen är absolut nödvändiga.
- **Fuktlarm** (vattenlarm, förekomst av vatten på golvet)
  Installera fuktlarm/vattenlarm i utrymmet.
- **Placera utrustningen upphöjt**
  Använd installationsgolv eller hyllor/rack/stativ för att lyfta upp utrustningen från golvet.
- **Rördragning**
  De rör som finns inne i ett it-utrymme bör vara placerade under installationsgolv eller monterade på väggar. Undvik montage i tak. Om rör monteras under installationsgolv, se till att luftcirkulationen inte påverkas.
- **Förstärkning**
  Kontrollera och inför förstärkning av rör. Det finns exempelvis möjligheter att kapsla in rör och på så sätt minska konsekvenserna av ett läckage.

20. Riksarkivet tillåter inte att rör för fjärrvärme och fjärrkyla finns i en arkivlokal. Inte heller andra typer av rör för vätskor får dras igenom en arkivlokal, med undantag för vattenledande rör för arkivlokalens uppvärmning och rör för arkivlokalens automatiska släcksystem. Rören för lokalens uppvärmning ska förläggas nära golvet. För att uppnå tillfredsställande skydd kan befintliga rörinstallationer kompletteras med avledande dropp- och uppsamlingsrännor. Vid risk för vattenläckage eller inträngande fukt bör myndigheten installera ett fuktlarm med signal till bemannad plats (RA-FS 2013:4, 6 kap. 2-3 §§).

- **Läckageskydd**
  Finns det rör som är installerade i utrymmets tak eller på väggar (nära it-utrustning och datamedia) – montera läckageskydd (plåtar, hängrännor eller liknande) under dessa rör och led bort eventuell vätska. Om möjligt, placera fuktlarm (vattenlarm) i skyddet.
- **Evakuering**
  Om läckage sker, se till att vätskan kan evakueras innan utrymmet översvämmas. It-utrymmen bör vara försedda med evakueringsbrunnar, speciellt de utrymmen som är belägna under markplan. Brunnarna ska vara försedda med backventiler och uttorkningsskydd. Alternativt kan de vara försedda med manuell öppna/stäng-funktion. Andra lösningar med pumpgropar kan också vara möjliga.
- **Vätsketät konstruktion**
  Lösningar finns på marknaden för att bygga ett it-utrymme vätsketätt. En vätsketät konstruktion kan användas om det finns omfattande risker för yttre vätskeläckage från stora volymer vätska och om möjligheterna för evakuering av vätska är små.
- **Övriga skydd**
  Varje it-utrymme är unikt och det finns ofta smarta lösningar och skydd som kan förbättra en till synes omöjlig situation. Om risker finns för läckage bör man alltid konsultera expertis inom området för att få förslag på lösningar.

Det är inte ovanligt att rör passerar genom utrymmen som är tilltänkta som it-utrymmen även i nybyggda fastigheter. Se därför till att involveras tidigt i dessa projekt för att minimera riskerna för vätskeläckage. Skyddsåtgärder kan annars medföra stora kostnader i efterhand.

## 2.8 Interiör i it-utrymmen

Hur ett it-utrymme inreds kan vara avgörande för att minimera risker för att negativa händelser inträffar. Val av material i ett it-utrymme har också en betydelse för att inte skapa incidenter eller förvärra en incident som redan har ägt rum.

### 2.8.1 Golv

Takhöjden i ett it-utrymme är oftast avgörande om ett installationsgolv (även kallat datagolv) kan installeras eller inte. Ett installationsgolv monteras ovanpå utrymmets befintliga golv, byggs upp av en stålställning och ovanpå ställningen läggs normalt kvadratiska plattor. Fördelen med ett installationsgolv är att fasta installationer som datakablar, elkablar och vätskerör till största delen kan förläggas under installationsgolvet. Det blir på så sätt enklare att hålla god ordning och reda i it-utrymmet och man minskar risker för incidenter. Dessutom kan man välja att distribuera kyld luft under installationsgolvet. Där kyla behövs, monteras ett galler i golvet istället för en täckt platta. Ytterligare en fördel med installationsgolv är att materialet i golvet ofta är antistatiskt och minskar därför riskerna för incidenter orsakade av statisk elektricitet. Alternativa lösningar till installationsgolv finns på marknaden och det är möjligt att uppnå en god säkerhet i ett it-utrymme utan denna funktion.

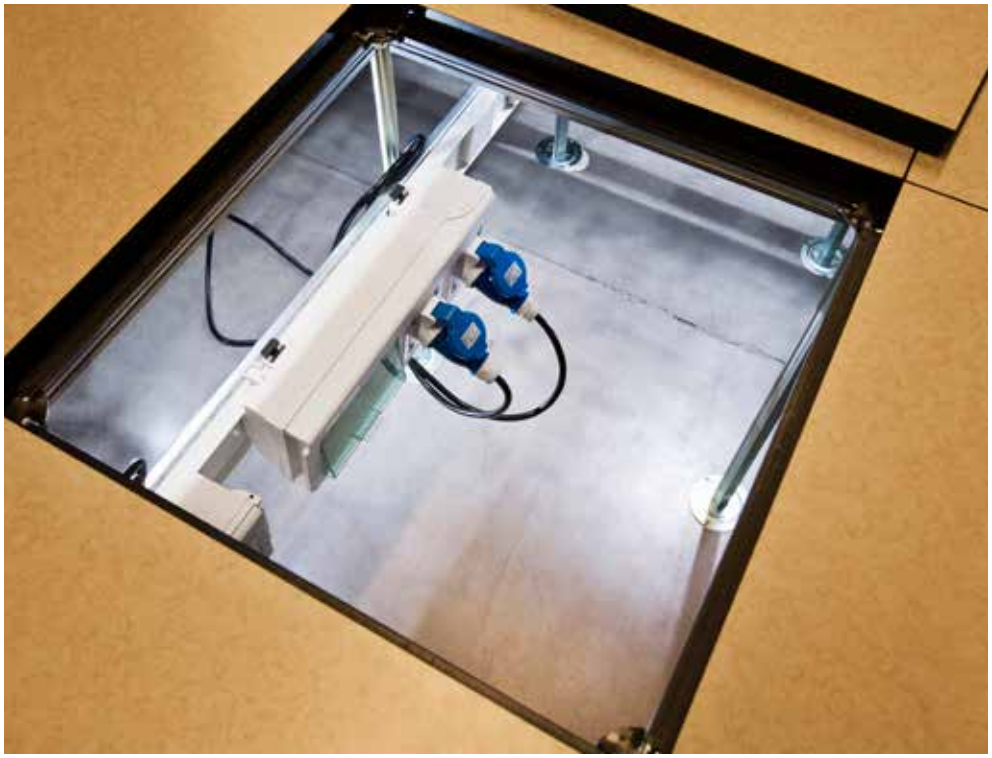


*Bild 19. El-matning till rack/stativ placerad under installationsgolv.*

Om takhöjden i ett it-utrymme medger installationsgolv, bör ett sådant installeras. Om man samtidigt avser att använda underblåsande kyla bör installationsgolvet monteras minst 400 mm över det befintliga golvet. Annars kan det finnas risk att man får svårt att distribuera tillräcklig luftmängd under golvet. Höjden på golvet är till viss del beroende av it-utrymmets yta: ju större yta, desto högre golv, upp till en viss gräns.

Avser man inte att använda underblåsande kyla bör montaget vara på minst 200 mm över befintligt golv, eftersom det annars riskerar att bli för trångt för installationer. Lyftanordningar för plattor ska monteras i utrymmet om installationsgolv används.

Finns det inget installationsgolv eller möjligheter saknas att installera ett bör man se till att det befintliga golvet behandlas för att minimera riskerna för att statisk elektricitet uppstår. Oavsett typ av golv bör det placeras en smutsavskiljare (normalt en klistermatta i flera lager, där översta lagret kan tas bort) på golvet direkt innanför ingången till utrymmet för att minska riskerna för att damm och smuts förs in i utrymmet.

### 2.8.2 Väggar och tak

Materialet i väggar och tak (och golv) styrs av den brandskyddsklass och inbrottsklass verksamheten väljer. Generellt gäller att man ska undvika brännbara material i golv-, vägg- och takyta. Väggar och tak bör helst målas i ljus färg för att underlätta arbeten i utrymmet. Konsultera gärna expertis för val av färgtyper.

### 2.8.3 Kanalisation

Alla installationer i ett it-utrymme bör förläggas på kabelstegar, under golvet om installationsgolv finns eller i hängande kabelstegar monterade i tak om installationsgolv saknas. Använd separata kabelstegar för datanät och elnät och kontrollera att dessa inte korsar varandra i direkt anslutning. Vid nyinstallationer bör man minst planera för en utbyggnad om 50 %, d.v.s. att kabelstegarna inte ska vara mer än till hälften fyllda. Vid underblåsande kyla under installationsgolv är det också viktigt att luftcirkulationen inte störs av kanalisationen, montera därför **aldrig** kabelstegar tvärs luftflödet.

*Bild 20. Kabelstegar monterade i tak.*

### 2.8.4 Genomföringar

Alla kablar och rörgenomföringar till ett it-utrymme ska vara brand- och tryckssäkra. Genomföringarna ska tätas enligt den brandskyddsklass som har tillämpats.

Om en verksamhet vet att man kommer genomföra förändringar i rör och kabeldragningar, kan flexibla genomföringar övervägas. Denna typ av produkt gör det möjligt att utöka/minska antalet genomföringar genom en modul-uppbyggd lösning.

### 2.8.5 Belysning

Som tidigare nämnts (i kapitel 2.6) ska belysning som är anpassad till tekniska utrymmen användas. Medelbelysningen bör vara anpassad efter de arbetsuppgifter som ska utföras i utrymmet. Finns det krav på nödbelysning och kontinuerligt lysande utgångsskyltar ska detta användas. Normalt räcker det dock att installera en säkerhetsbelysning vilket inte medför samma strikta krav på installation, men erbjuder i huvudsak samma funktion som nödbelysning (se avsnitt 2.6.1).

### 2.8.6 Montage av it-utrustning

Numera är den vanligaste typen av montage i it-utrymmen rack eller stativ. Hyllor med stående servertyper (tower-modeller) används dock fortfarande i vissa verksamheter. En av de viktigaste aspekterna med montage är att utrustningen monteras upplyft från golvet. Riskerna för negativa incidenter från exempelvis vätska minskar generellt med upplyft montage och det ger en förbättrad luftcirkulation.

I rack och stativ bör it-utrustning monteras så att luftcirkulationen inte påverkas negativt och varma zoner bildas. En alltför tät montering kan leda till värmeproblem. Se också till att kablar för el och data monteras på sådant sätt att luftcirkulationen inte påverkas negativt.

### 2.8.7 Möbler

Många it-utrymmen innehåller möbler för att personal ska kunna arbeta ergonomiskt riktigt. Skrivbord, hurtsar, hyllor och stolar är därför relativt vanligt förekommande. Det bästa alternativet är att försöka undvika användning av möbler i it-utrymmen generellt och placera arbetsplatser och olika typer av förvaringar utanför utrymmet, exempelvis i en sluss som tidigare har diskuterats.

Måste möbler användas i it-utrymmen ska dessa vara tillverkade av ett material som inte är brännbart. Det finns möbler på marknaden som är speciellt utformade för känsliga tekniska utrymmen (se även 2.4 Brandskydd).

### 2.8.8 Märkning

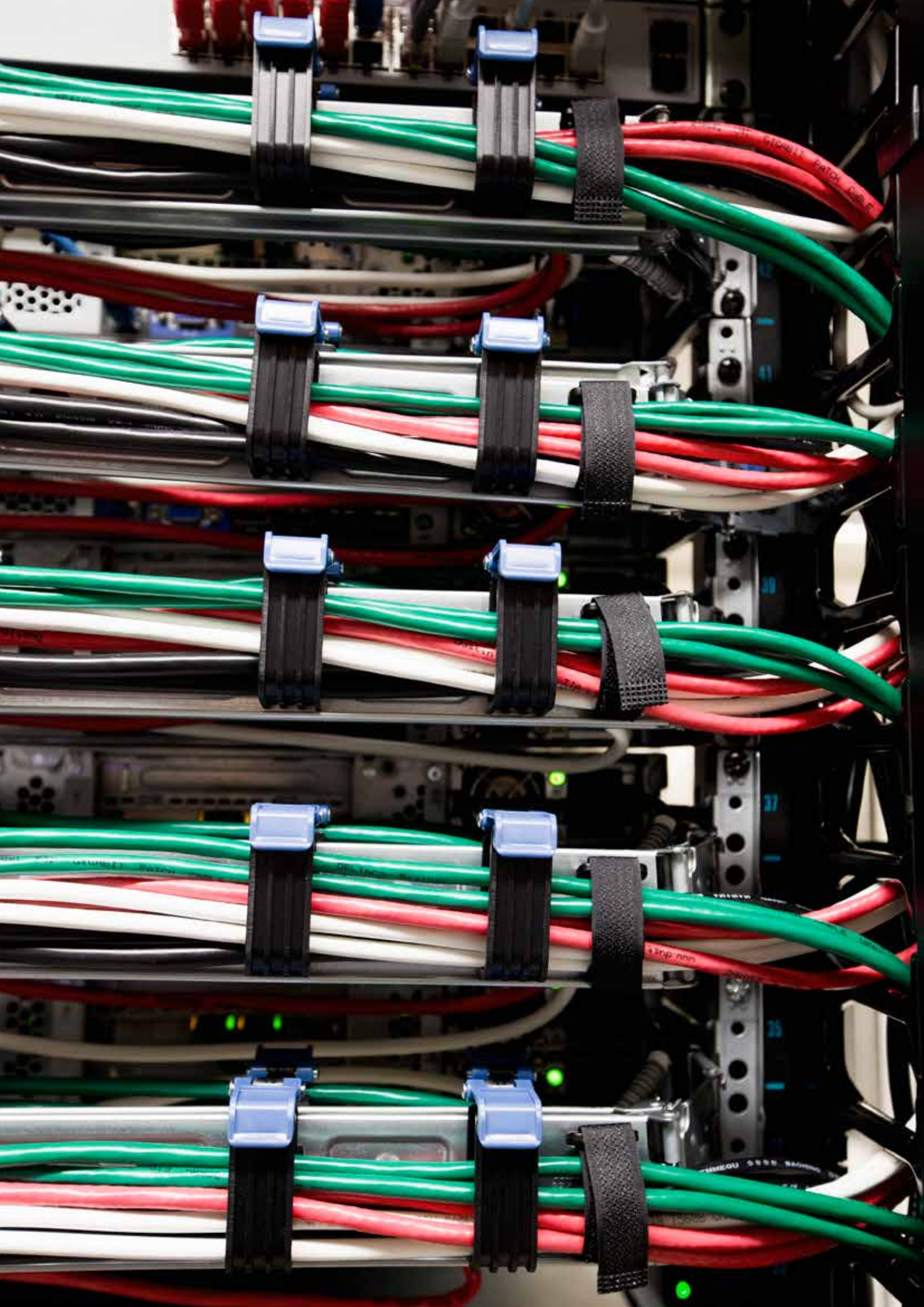
Alla kablar, it-utrustningar och uttag i ett it-utrymme ska märkas med ett varaktigt märkningssystem. Det finns både svenska och europeiska normer som kan tillämpas. Man bör försöka använda skyltar för märkning som sätts fast med skruvar, nitar eller buntband istället för tejpmärkning som enkelt kan lossna. Undvik att placera märkning på täckplåtar, fronter, lock eller liknande som kan försvinna. I genomföringar i brandcellen är det viktigt att se till att märkningen sker på båda sidor av genomföringen.

Förutom märkning, använd gärna olika färger på kablar i korskopplingar och anslutning av it-utrustningar för att förenkla arbetet och skapa god ordning, exempelvis röda datakablar för oskyddad internettrafik, blå kablar för telefoni och gröna kablar för intern skyddad datatrafik.

## 2.9 Teknisk övervakning och larm

Det finns fler tekniska utrustningar i ett it-utrymme än bara servrar och switchar. It-utrymmets tekniska infrastruktur har en stödjande funktion för it-miljön för att exempelvis hantera strömavbrott eller kontrollera temperatur. Uppstår fel i dessa utrustningar måste någon meddelas annars riskerar it-utrustning och datamedia att skadas. Teknisk övervakning och driftlarm är nödvändigt.

***Bild 21 (till vänster).*** *Brandtätning av genomföring i brandcellsgräns. Observera att någon utökat genomföringen i detta fall och inte återtätat korrekt.*



### Övervakning och åtgärd

All teknisk infrastruktur i ett it-utrymme bör förses med larmfunktioner, ett driftlarm. Ett driftlarm är ett summalarm som normalt är anslutet till övriga fastighetsrelaterade larm. Möjligheter finns också normalt att föra vidare larm till andra övervakningssystem eller ansluta till larmöverföring mot exempelvis bevakningsorganisation eller serviceorganisation.

Den säkraste vägen att skicka ett larm från ett it-utrymme är till en bevakningsorganisation som i sin tur vidarebefordrar larmet eller ringer en utsedd kontaktperson. Detta ger en relativt hög säkerhet i larmmottagningen, till en låg kostnad. Automatiska larm via sms (som används i vissa verksamheter idag) ger generellt en för låg säkerhet eftersom man riskerar att de inte läses.

På senare år har det blivit möjligt att ansluta driftlarmscentraler via it-baserade gränssnitt. Eftersom många verksamheter har it-baserad övervakning idag kan man även övervaka infrastrukturen i it-utrymmen. Eftersom strukturen för larm till personal och serviceorganisationer oftast redan är implementerad i dessa system, är tillägg av driftlarm ett mindre arbete.

### Typer av larm och begrepp

Följande begrepp och typer av larm är vanliga i it-utrymmen:

- **Driftlarm**
  Summalarm dit all infrastruktur ansluts.
- **Inbrottslarm**
  Separat larm för att upptäcka obehörigt tillträde som normalt inte är anslutet till driftlarm. Fellarm från inbrottslarmutrustning skickas normalt till bevakningsorganisation, men kan även skickas till driftlarm.
- **Brandlarm**
  Om it-utrymmet har eget brandlarm är detta normalt i sin tur anslutet till fastighetens brandlarm. Fellarm från brandlarmet kan dock anslutas till driftlarmet.
- **Temperaturlarm (luftfuktighet)**
  Övervakar temperatur och luftfuktighet. Larmet är normalt endast anslutet till driftlarmet.
- **Fuktlarm (vattenlarm, förekomst av vatten på golvet)**
  Larm för att upptäcka vätskeläckage. Larmet är normalt endast anslutet till driftlarmet.
- **Kyla**
  Larm för att upptäcka fel på någon komponent i kylanläggningen. Larmet är normalt endast anslutet till driftlarmet. Aktivering av nödkyla ger också larm.
- **Reservkraft**
  Larm för att upptäcka fel på reservkraftanläggningen eller upptäcka om anläggningen har aktiverats. Larmet är normalt endast anslutet till driftlarmet.

***Bild 22 (till vänster).*** *Användning av kablar i olika färger skapar ordning och förenklar arbetet i it-utrymmet.*

- **UPS**
  Larm för att upptäcka fel på UPS-enheter eller upptäcka om anläggningen har aktiverats. Larmet är normalt endast anslutet till driftlarmet.
- **Övriga larm eller manövrar**
  All teknisk utrustning som har gränssnitt för att kommunicera med driftlarmet kan anslutas.

Det är extremt viktigt att alla tekniska larm, driftlarm etc. har en robust konstruktion med egna batterier för drift i spänningslöst tillstånd. Alla larm ska kunna skickas oavsett tillståndet i it-utrymmet (exempelvis strömavbrott, haveri i datakommunikationsförbindelser eller andra liknande störningar).

# Bilaga 1

# Bilaga 1 – Exempel på skyddsnivåer

All information har inte behov av samma skydd. Informationsklassning är stödet för att identifiera rätt skyddsnivå för olika informationsmängder. Skyddsnivåerna måste beskrivas så att de kan implementeras både av interna och externa leverantörer. För att ge stöd för att ta fram skyddsnivåer följer här exempel på hur de kan utformas inom fysisk säkerhet. Observera att det är informationens skyddsvärde som styr vilken skyddsnivå som bör användas. Det går alltså inte att säga att en datorhall alltid ska ligga på skyddsnivå 3 och ett korskopplingsutrymme på skyddsnivå 1. Att använda sig av skyddsnivåer kan dock leda till att en organisation även av ekonomiska skäl försöker systematisera sitt fysiska skydd. Det innebär bland annat att försöka sammanföra utrustning som innehåller information med samma skyddsvärde till samma utrymmen för att undvika att behöva införa dyra skyddsåtgärder för enstaka utrustningar.

Varje skyddsnivå har tilldelats ett eget avsnitt som kan användas som en mall för ett utrymme av motsvarande typ. Skyddsnivåer kan vara liknande eller likadana inom flera delområden. Samtliga delområden och relaterade skydd redovisas dock per nivå och upprepas därför om ingen förändring har skett från föregående nivå.

**Observera att detta bara är exempel och att varje organisation måste göra bedömningar av sina unika förutsättningar.**

Tre skyddsnivåer kommer att användas i detta kapitel vilka kopplas till en typ av it-utrymmen enligt följande princip:

- **Skyddsnivå 3, typ datorhall**
  Med en datorhall avses en lokal som förvarar en större mängd it-utrustningar. Lokalen är initialt avsedd och projekterad för it-drift.
- **Skyddsnivå 2, typ datorrum**
  Med datorrum avses en lokal som förvarar en mindre mängd it-utrustningar. Lokalen kan vara anpassad för it-drift, men är inte uttalat avsedd eller projekterad för det ändamålet.
- **Skyddsnivå 1, typ kommunikations-/KK-rum**
  Ett KK-rum är en lokal där kommunikationsutrustningar såsom routers, switchar och hubbar kopplas samman. Lokalen kan vara anpassad för it-drift. I ett KK-rum förvaras ingen utrustning som innehåller datamedia (hårddiskar, databand, disketter eller liknande).

Varje skyddsnivå har tilldelats ett eget avsnitt som kan användas som en mall för ett utrymme av motsvarande typ. Observera att skyddsnivåerna och typerna av it-utrymmen är en generalisering. Ska nivå och typ användas i ”skarpa” tillämpningar ska en anpassning till aktuell verksamhets verkliga förutsättningar, omvärldskrav och förväntningar genomföras.

Observera att allmänna handlingar, utifrån ett arkiv- och bevarandeperspektiv, inte kan värderas olika med utgångspunkt i informationsinnehåll. Myndigheten har ett ansvar att följa tillämpliga arkivregler och se till att varje handling, oavsett informationsinnehåll, ges ett tillfredsställande skydd under hela bevarandetiden. De skyddskrav som anges i denna bilaga överensstämmer inte alltid med de krav som Riksarkivet ställer. Nedanstående skyddsnivåer kan ändå utgöra en checklista vid planering av it-utrymmen. Riksarkivets krav måste dock alltid tas hänsyn till i de fall allmänna handlingar förvaras i it-utrymmet.

## Skyddsnivå 3 (typ datorhall)

- **Placering**
  Utrymmet ***ska inte*** placeras i omedelbar anslutning till våtutrymmen eller större elektromagnetiska källor, exempelvis hissmaskinrum. Placering vid yttervägg samt under markplan ***bör*** undvikas. Utrymmet ***ska*** vidare inte placeras i närheten av förvaring av brandfarligt material eller i närheten av förvaring av brännbara material som kan agera katalysator vid en eventuell brand, t.ex. kontorsförråd. Utrymmet ***bör*** placeras minst en våning över markplan. Omkringliggande vattendrag eller andra risker för inströmmande vätska ***ska*** tas hänsyn till.
- **Byggnation och skalskydd**
  Utrymmet ***ska minst*** uppfylla kraven i SSF 200, skyddsklass 3 för konstruktion, fastsättning av golv, väggar, tak och dörrar. Samtliga väggar ***ska*** ansluta tätt till golv och tak. Fönster ***ska inte*** finnas i utrymmet. Det ***bör*** finnas operatörsrum/arbetsrum i anslutning till utrymmet (lämpligen i en sluss).
- **Brandskydd**
  Utrymmet ***ska*** utgöra en egen brandcell och uppfylla brandteknisk klass minst EI60 men ***bör*** uppfylla brandteknisk klass EI-120. Vid svårigheter att minimera brandbelastning eller motsvarande situationer ***ska*** högre brandtekniska klasser som exempelvis R60/90D utredas.
- **Golv**
  Installationsgolv med antistatisk matta (även kallat datagolv) ***ska*** användas, med en höjd på minst 400 mm över underliggande golv. Det ***ska*** finnas lyftanordningar för att möjliggöra släckning av kabelbränder under golv. Det ***bör*** finnas fluorescerande riktningsmarkeringar på golven som visar vägen till utrymningsutgångar.
- **Tak**
  Ljudabsorbenter eller undertak ska undvikas för att inte binda eller samla damm.
- **Dörrar**
  Utrymmet ***ska*** vara utformat med en sluss om två dörrar. Slussen ***ska*** ha en yta om minst fem till sex kvadratmeter, för att tillåta förvaring av papper/böcker/manualer/licenser eller annat brännbart material som ***inte ska*** förvaras inne i utrymmet. Ståldörrar som minst uppfyller motståndsklass 4 enligt SS EN1627 samt utrymmets brandtekniska klass (se brandskydd) ***ska*** användas. Alla dörrar

***ska*** av utrymningsskäl öppnas utåt. Låscylindrar ***ska*** ingå i den egna verksamhetens låssystem. Låsningen ***ska*** vara separerad på sådant sätt att endast behörig personal bereds tillträde.

- **Tillträde**
  Tillträde ***ska*** endast vara tillåtet för behörig personal. Tillträdeskontroll ***ska*** ske genom passagekontrollsystem med loggfunktion.
- **Inbrottslarm**
  Alla dörrar ***ska*** vara larmade och larmen kopplade till verksamhetens ordinarie larm-övervakning. Utrymmet ***ska*** utgöra ett eget larmområde enligt SSF 130, minst larmklass 2, larmklass 3 ***bör*** användas.
- **Nödsignal, överfallslarm**
  Det ***bör*** finnas lättåtkomliga olycksfalls- och överfallslarm inom utrymmet vilka är anslutna till verksamhetens ordinarie larmövervakning.
- **El**
  Elkraftssystemen som försörjer utrymmet ska vara av typen 5-ledarsystem. Två separata elkraftsmatningar inklusive huvudbrytare och centraler ***bör*** användas. Överspänningsskydd ska finnas för all infrastruktur i utrymmet såsom elkraftsförsörjning, kylanläggning och telekommunikation.

  Reservkraft ***ska*** finnas. Reservkraft ***ska*** även mata klimatanläggning, belysning samt allmänkraft i utrymmet.

  Varje stativ för it-utrustning ***ska*** förses med avbrottsfri kraft (UPS), minst två separata grupper per stativ med 2 X 16A trefas på handske. UPS av typen on-line ***ska*** användas. En riskanalys ***ska*** göras för att fastställa om dubbla UPS behövs. Varje UPS (om dubblerad) ***bör*** ha sitt eget batteri. Belysningen, övriga eluttag eller annan allmänkraft i utrymmet ***ska*** matas från en grupp som är skild från UPS. Separat avsäkrade fördelare (PDU) ***ska*** användas i stativ.

  Batterier för UPS ***bör*** vara ventilreglerade och ***bör*** ha en förväntad livslängd på minst 10 år. Batterierna ***ska*** vara dimensionerade för att säkerställa el under den tid som åtgår för kontrollerad avstängning av utrustningen alternativt manuell start av reservkraft, dock minst 10 minuter och maximalt 30 minuter. Batterierna ***bör*** placeras på en fristående ställning men kan även vara integrerade i UPS-anläggningen. Observera att öppna batterier kräver ett eget utrymme samt att batteripaket kan ge stor punktlast vilket kan kräva förstärkningar av golv.

  Riskanalyser ***ska*** utföras för att fastställa elanläggningarnas behov av kompletterande åtgärder.
- **EMP (elektromagnetisk strålning)**
  Behovet av skydd mot elektromagnetisk strålning ***ska*** utredas.
- **Belysning**
  Medelbelysningsnivå ***bör*** vara 500 lux. Lysrörsarmaturer anpassade till känsliga miljöer ***ska*** användas. Utrymmet ***ska*** utrustas med säkerhetsbelysning som dimensioneras för funktion under minst en timme. Eventuella utgångsskyltar ***ska*** lysa kontinuerligt. Behovet av nödbelysning ***ska*** utredas.
- **Korskoppling**
  Korskopplingar för allmänt datanät i fastigheten ***bör*** inte finnas i utrymmet, utan placeras till separata utrymmen.

- **Kanalisation**
  Separata kabelstegar för el- och datanät ***ska*** användas. Vid nyanläggning ***ska*** 50 % reservutrymme för utbyggnad och komplettering planeras.
- **Genomföringar**
  Alla kabel- och rörgenomföringar ***ska*** vara brandtätade enligt utrymmets brandtekniska klass (se brandskydd). Användning av flexibla genomföringar ***ska*** övervägas.
- **Montage**
  Rackmontage ***ska*** användas.
- **Separata placeringar**
  It-utrustning för säkerhetskopiering ***ska*** placeras i en brandcell som är skild ifrån it-utrustning som lagrar primärdata. Reservkraft och utrustning för automatiska släcksystem samt klimatanläggning ***ska*** placeras i separata utrymmen.
- **Vätska**
  Rörledningar och övriga installationer som innehåller vätska, utöver de som är nödvändiga för klimatregleringen, ***ska inte*** finnas i utrymmet. Dragning av rörledningar ***ska*** i största möjliga mån göras under installationsgolv. Om vätskeinstallationer finns i utrymmet ***ska*** avloppsbrunnar finnas. Anläggning av avloppsbrunn ***ska*** även övervägas vid låg placering och vid risk för inströmmande vätska. Avloppsbrunnar ***ska*** ha skydd mot uttorkning och mot uppstigande vätska. Fuktlarm ***ska*** finnas och larmet ***ska*** vara anslutet till verksamhetens ordinarie larmövervakning.
- **Klimat**
  Utrymmets temperatur ***ska*** inte tillåtas variera utanför temperaturgränserna +18 °C till +23 °C. Utrymmet ***ska*** förses med ventilations- och kylanordning (av typ precisionskyla). Underblåsande kyla ***ska*** användas. Ventilations- och/eller klimatanläggning ***ska*** producera ett övertryck. Temperaturlarm, kopplat till verksamhetens ordinarie larmövervakning, ***ska*** finnas. En anordning för reglering av utrymmets luftfuktighet ***ska*** användas. Risker för vätskeläckage från kylanordning ***ska*** tas hänsyn till.

  Tilluft samt luft som passerar klimatutrustning ***ska*** filtreras. Dessa filter ***ska*** bytas regelbundet. Tilluftskanaler ***ska*** förses med rökdetektorer anslutna till brandspjäll eller automatiska fläktstopp. Luftomsättningen ***ska*** dimensioneras utifrån arbetsmiljökraven för att det antal personer som är tänkta att kunna vistas kontinuerligt i utrymmet. Nödkyla (ytterligare köldbärare) ***ska*** finnas tillgänglig för att säkerställa kontinuerlig drift. Kyleffekten hos kylanordningen för utrymmet ***ska*** utredas men ***bör*** dimensioneras med minst 2 kilowatt per kvadratmeter yta i utrymmet.
- **Brand**
  Brandlarm med egen larmsektion som är kopplat till verksamhetens ordinarie brandlarmsövervakning ***ska*** finnas. Det ***ska*** finnas handbrandsläckare (typ av släckmedel som ***inte*** skadar it-utrustning), innehållande minst 5 kilo släckmedel, både på utsidan av utrymmet i nära anslutning till ordinarie ingång samt inne i utrymmet. Om ventilationsanläggning finns, ***ska*** ventilationskanaler förses med brandspjäll kopplade till brandlarm. Utrymmet ***ska*** förses med ett automatiskt brandsläckningssystem med aspirerande/samplande branddetektering. Samtliga dörrar ***ska*** förses med panikregel på insidan. Material inne i utrymmet ***ska inte*** vara brännbart. Detta gäller t.ex. hyllor, stativ, skåp eller andra montage eller möbler som används.

- **Sektionering**
  Utrymmet ***bör*** efter behov kunna sektioneras, exempelvis för utrustning med olika krav på tillträdesskydd eller skalskydd. Om sektionering används ***ska*** alla områden avskärmas, inklusive krypgrunder, ventilationsgångar och under installationsgolv. Sektionering ***ska*** uppfylla de krav som ställs för skyddsklass 2 i SSF 200. Observera att sektionering också kan utföras för att skapa separata brandceller i utrymmet för att på så sätt minska kraven på släckanläggningens storlek och mängden släckmedel.
- **Skyltning**
  Skyltning utanför utrymmet som avslöjar utrymmets funktion eller innehåll ***ska*** undvikas. Rutiner/regler som gäller för utrymmet ***bör*** skyltas tydligt inne i utrymmet.
- **Märkning**
  All utrustning ***ska*** märkas med varaktigt märksystem. Alla skyltar ***ska*** sättas fast med skruv, nit eller band. Alla hållare för utbytbar märkning ***ska*** sättas fast med motsvarande metod. All märkning ***ska*** byggas upp med anläggningsnummer i kombination med text eller löpnummer. Märkningen ***ska*** inte följa med exempelvis täcklock eller frontplåt när dessa avlägsnas. Märkning ***ska*** göras på samtliga ledningar vid centralutrustning, vid anslutningsobjekt samt vid varje passage av överspänningsskydd eller brandcellsgräns samt valv- och markgenomgång.
- **Ledningar och kablar**
  Kabelgravar utanför skalskyddsgränsen ***bör*** undvikas. Kabelbrunnar ***bör*** förses med lås. Jordnings- och potentialskillnadsproblem ***ska*** ägnas stor uppmärksamhet, speciellt om anläggningen ***ska*** anslutas till befintlig kanalisations- och kabelinfrastruktur.
- **Insatsplaner och utrymningsplaner**
  Alla utrymmen ***ska*** ha en giltig och uppdaterad insatsplan för brand, vätskeläckage, sabotage eller andra tillbud (definierade i riskanalys). Insatsplanen för brand ***ska*** uppfylla SBF 100 och ***bör*** uppfylla kraven i SBF 110.

## Skyddsnivå 2 (typ datorrum)

- **Placering**
  Utrymmet ***ska*** inte placeras i omedelbar anslutning till våtutrymmen eller större elektromagnetiska källor, exempelvis hissmaskinrum. Placering vid ytterväggg ***ska*** undvikas och placering under markplan ***bör*** undvikas. Utrymmet ***ska*** vidare inte placeras i närheten av förvaring av brandfarligt material eller i närheten av förvaring av brännbara material som kan agera katalysator vid en eventuell brand, t.ex. kontorsförråd. Utrymmet ***bör*** placeras minst en våning över markplan. Omkringliggande vattendrag eller andra risker för inströmmande vätska ***ska*** tas hänsyn till.
- **Byggnation och skalskydd**
  Utrymmet ***ska*** uppfylla kraven i SSF 200:3, skyddsklass 2 för konstruktion, fastsättning av golv, väggar, tak och dörrar. Samtliga väggar ***ska*** ansluta tätt till golv och tak. Fönster ***ska inte*** finnas i utrymmet.
- **Brandskydd**
  Utrymmet ***ska*** utgöra en egen brandcell och uppfylla brandteknisk klass EI60.

- **Golv**
  Installationsgolv med antistatisk matta (även kallat datagolv) ***bör*** användas, med en höjd på minst 400 mm över underliggande golv. Om installationsgolv inte används ska en antistatisk golvbeläggning användas.

- **Dörrar**
  Utrymmet ***bör*** vara utformat med en sluss om två dörrar. Slussen ***bör*** ha en yta om minst fem till sex kvadratmeter, för att tillåta förvaring av papper/böcker/manualer/licenser eller annat brännbart material som inte ***bör*** förvaras inne i utrymmet. Förstärkta dörrar (ståldörrar) som minst uppfyller brandteknisk klass EI60 ***ska*** användas. Alla dörrar ***ska*** av utrymningsskäl öppnas utåt. Låscylindrar ***ska*** ingå i den egna verksamhetens låssystem. Låsningen ***ska*** vara separerad på sådant sätt att endast behörig personal bereds tillträde.

- **Tillträde**
  Tillträde ***ska*** endast vara tillåtet för behörig personal. Tillträdeskontroll ***ska*** ske genom passagekontrollsystem med loggfunktion.

- **Inbrottslarm**
  Alla dörrar ***ska*** vara larmade och larmen kopplade till verksamhetens ordinarie larmövervakning. Utrymmet ska utgöra ett eget larmområde enligt SSF 130, larmklass 2.

- **El**
  Varje stativ för it-utrustning ***ska*** förses med avbrottsfri kraft (UPS), minst två separata grupper per stativ. Belysningen, övriga eluttag eller annan allmänkraft ***ska*** matas från en grupp som är skild från stativuttagens matning. Separat avsäkrade fördelare ***bör*** användas i stativ. Riskanalyser ***ska*** utföras för att fastställa anläggningarnas behov av kompletterande åtgärder, reservkraft, överspänningsskydd etc.

  Batterier för UPS ***bör*** vara ventilreglerade och ***bör*** ha en förväntad livslängd på minst 10 år. Batterierna ***ska*** vara dimensionerade för att säkerställa el under den tid som åtgår för kontrollerad avstängning av utrustningen alternativt manuell start av eventuell reservkraft, dock minst 10 minuter och maximalt 30 minuter. Batterierna ***bör*** placeras på en fristående ställning men kan även vara integrerade i UPS-anläggningen. Observera att öppna batterier kräver ett eget utrymme samt att batteripaket kan ge stor punktlast vilket kan kräva förstärkningar av golv.

- **Belysning**
  Medelbelysningsnivå ***bör*** vara 500 lux. Lysrörsarmaturer med glimtändare ***ska*** undvikas.

- **Kanalisation**
  Separata kabelstegar för el- och datanät ***ska*** användas. Vid nyanläggning ***ska*** 30 % reservutrymme för utbyggnad och komplettering planeras.

- **Genomföringar**
  Alla kabel- och rörgenomföringar ***ska*** vara brandtätade enligt brandteknisk klass EI60.

- **Montage**
  Samtlig it-utrustning ***ska*** vara placerad minst 10 cm över golvet. Rackmontage ***bör*** användas.

- **Vätska**
  Rörledningar och andra installationer som innehåller vätska ***bör*** inte finnas i utrymmet. Om sådana finns ***ska*** dessa i största möjliga mån lokaliseras till väggar och ***ska*** inte passera över eller i närheten av utrustnar i utrymmet. Om vätskeinstallationer finns i utrymmet ***ska*** avloppsbrunnar finnas. Anläggning av avloppsbrunn ***ska*** även övervägas vid låg placering och vid risk för inströmmande vätska. Avloppsbrunnar ***ska*** ha skydd mot uttorkning och mot uppstigande vätska. Fuktlarm ***ska*** finnas och larmet ***ska*** vara anslutet till verksamhetens ordinarie larmövervakning.

- **Klimat**
  Utrymmets temperatur ***ska*** inte tillåtas variera utanför temperaturgränserna +18 °C till +25 °C. Utrymmet ***ska*** förses med ventilations- och kylanordningar. Ventilations- och/eller klimatanläggning ***bör*** producera ett övertryck. Temperaturlarm, kopplat till verksamhetens ordinarie larmövervakning, ***ska*** finnas. Anordning för reglering av utrymmets luftfuktighet ***ska*** användas. Risker för vätskeläckage från kylanordning samt risker för strömavbrott ***ska*** tas hänsyn till. En kylanordning matas inte med avbrottsfri kraft och kan därför behöva tillgång till reservkraft.

  Kyleffekten hos kylanordningen för utrymmet ***ska*** utredas men ***bör*** dimensioneras med minst 1,5 kilowatt per kvadratmeter yta i utrymmet.

- **Brand**
  Brandlarm med egen larmsektion som är kopplat till verksamhetens ordinarie brandlarmsövervakning ***ska*** finnas. Det ***ska*** finnas handbrandsläckare (typ av släckmedel som ***inte*** skadar it-utrustning), innehållande minst 5 kilo släckmedel, på utsidan av utrymmet i nära anslutning till dörren. Om ventilationsanläggning finns ***ska*** ventilationskanalerna förses med brandspjäll kopplade till brandlarm. Utrymmet ***bör*** förses med ett automatiskt brandsläckningssystem och aspirerande/samplande branddetektering. Observera att om utrymmet förses med automatiskt brandsläckningssystem ***ska*** samtliga dörrar förses med panikregel på insidan. Material inne i utrymmet ***ska inte*** vara brännbart. Detta gäller t.ex. hyllor, stativ, skåp eller andra montage eller möbler som används.

- **Skyltning**
  Skyltning utanför utrymmet som avslöjar utrymmets funktion eller innehåll ***ska*** undvikas. Rutiner/regler som gäller för utrymmet ***bör*** skyltas tydligt inne i utrymmet.

- **Märkning**
  All utrustning ***ska*** märkas med varaktigt märksystem. Alla skyltar ***ska*** sättas fast med skruv, nit eller band. Alla hållare för utbytbar märkning ***ska*** sättas fast med motsvarande metod. All märkning ***ska*** byggas upp med anläggningsnummer i kombination med text eller löpnummer. Märkning ***ska*** inte följa med exempelvis täcklock eller frontplåt när dessa avlägsnas. Märkning ***ska*** ske på samtliga ledningar vid centralutrustning, vid anslutningsobjekt samt vid varje passage av överspänningsskydd eller brandcellsgräns samt valv- och markgenomgång.

- **Ledningar och kablar**
  Kabelgravar utanför skalskyddsgränsen ***bör*** undvikas. Kabelbrunnar ***bör*** förses med lås. Jordnings- och potentialskillnadsproblem ***ska*** ägnas stor uppmärksamhet, speciellt om anläggningen ***ska*** anslutas till befintlig kanalisations- och kabelinfrastruktur.

- **Insatsplaner och utrymningsplaner**
  Alla utrymmen ***ska*** ha en giltig och uppdaterad insatsplan för brand, vätskeläckage, sabotage eller andra tillbud (definierade i riskanalys). Insatsplanen för brand ***ska*** uppfylla SBF 100 och ***bör*** uppfylla kraven i SBF 110.

## Skyddsnivå 1 (typ kommunikations-/KK-rum)

- **Placering**
  Utrymmet ***ska inte*** placeras i omedelbar anslutning till våtutrymmen eller större elektromagnetiska källor, exempelvis hissmaskinrum. Placering vid ytterväggg och under markplan ***bör*** undvikas. Utrymmet ***ska*** vidare inte placeras i närheten av förvaring av brandfarligt material eller i närheten av förvaring av brännbara material som kan agera katalysator vid en eventuell brand, t.ex. kontorsförråd. Utrymmet ***bör*** placeras minst en våning över markplan. Omkringliggande vattendrag eller andra risker för inströmmande vätska ***ska*** tas hänsyn till.
- **Byggnation och skalskydd**
  Utrymmet ***ska minst*** uppfylla kraven i SSF 200, skyddsklass 1 men **bör** uppfylla skyddsklass 2 för konstruktion, fastsättning av golv, väggar, tak och dörrar.
- **Brandskydd**
  Utrymmet ***ska*** utgöra en egen brandcell och uppfylla brandteknisk klass EI60.
- **Golv**
  Antistatisk golvbeläggning ***ska*** användas.
- **Dörrar**
  Förstärkta dörrar (ståldörrar) som minst uppfyller brandteknisk klass EI60 ***ska*** användas. Alla dörrar ***ska*** av utrymningsskäl öppnas utåt. Låscylindrar ***ska*** ingå i den egna verksamhetens låssystem. Låsningen ***ska*** vara separerad på sådant sätt att endast behörig personal bereds tillträde.
- **Tillträde**
  Tillträde ***ska*** endast vara tillåtet för behörig personal. Tillträdeskontroll ***bör*** ske genom passagekontrollsystem med loggfunktion.
- **Inbrottslarm**
  Alla dörrar ***ska*** vara larmade och larmen kopplade till verksamhetens ordinarie larmövervakning.
- **El**
  Varje stativ ***bör*** förses med 2-vägsuttag som ***ska*** vara anslutna via separata grupper. Eluttag i stativ ***ska*** matas via avbrottsfri kraft (UPS). Belysningen, övriga eluttag eller annan allmänkraft ***ska*** matas från en grupp som är skild från UPS.

  Riskanalyser ***ska*** utföras för att fastställa elanläggningarnas behov av kompletterande åtgärder, UPS, reservkraft, överspänningsskydd etc.
- **Belysning**
  Medelbelysningsnivå ***bör*** vara 500 lux. Lysrörsarmaturer med glimtändare ***ska*** undvikas.
- **Kanalisation**
  Separata kabelstegar för el- och datanät ***ska*** användas. Vid nyanläggning ***ska*** 30 % reservutrymme för utbyggnad och komplettering planeras.

- **Genomföringar**
  Alla kabel- och rörgenomföringar ***ska*** vara brandtätade enligt brandteknisk klass EI60.

- **Vätska**
  Rörledningar och andra installationer som innehåller vätska ***bör*** inte finnas i utrymmet. Om sådana finns ***ska*** dessa i största möjliga mån lokaliseras till väggar och ***ska*** inte passera över eller i närheten av utrustning i utrymmet. Om vätskeinstallationer finns i utrymmet ***ska*** avloppsbrunnar finnas. Anläggning av avloppsbrunn ***ska*** även övervägas vid låg placering och vid risk för inströmmande vätska. Avloppsbrunnar ***ska*** ha skydd mot uttorkning och mot uppstigande vätska.

- **Klimat**
  Utrymmets temperatur ***ska*** inte tillåtas variera utanför temperaturgränserna +18 °C till +25 °C, detta kan kräva ventilations- och kylanordningar. Ventilations- och/eller klimatanläggning ***bör*** producera ett övertryck. Temperaturlarm, kopplat till verksamhetens ordinarie larmövervakning, ***ska*** finnas. Anordning för reglering av utrymmets luftfuktighet ***bör*** användas.

- **Brand**
  Brandlarm ***ska*** finnas. Det ***ska*** finnas handbrandsläckare (typ av släckmedel som ***inte*** skadar it-utrustning), innehållande minst 5 kilo släckmedel, på utsidan av utrymmet i nära anslutning till dörren. Om ventilationsanläggning finns ***ska*** ventilationskanalerna förses med brandspjäll kopplade till brandlarm.

- **Skyltning**
  Skyltning utanför utrymmet som avslöjar utrymmets funktion eller innehåll ***ska*** undvikas. Rutiner/regler som gäller för utrymmet ***bör*** skyltas tydligt inne i utrymmet.

- **Märkning**
  All utrustning ***ska*** märkas med varaktigt märksystem. Alla skyltar ***ska*** sättas fast med skruv, nit eller band. Alla hållare för utbytbar märkning ***ska*** sättas fast med motsvarande metod. All märkning ***ska*** byggas upp med anläggningsnummer i kombination med text eller löpnummer. Märkningen ***ska*** inte följa med exempelvis täcklock eller frontplåt när dessa avlägsnas. Märkning ***ska*** ske på samtliga ledningar vid centralutrustning, vid anslutningsobjekt samt vid varje passage av överspänningsskydd eller brandcellsgräns samt valv- och markgenomgång.

- **Ledningar och kablar**
  Kabelgravar utanför skalskyddsgränsen ***bör*** undvikas. Kabelbrunnar ***bör*** förses med lås. Jordnings- och potentialskillnadsproblem ***ska*** ägnas stor uppmärksamhet, speciellt om anläggningen ***ska*** anslutas till befintlig kanalisations- och kabelinfrastruktur.

- **Insatsplaner och utrymningsplaner**
  Alla utrymmen ***ska*** ha en giltig och uppdaterad insatsplan för brand, vätskeläckage, sabotage eller andra tillbud (definierade i riskanalys). Insatsplanen för brand ***ska*** uppfylla SBF 100 och ***bör*** uppfylla kraven i SBF 110.

# Bilaga 2

# Bilaga 2 – Checklista för lämpliga rutiner i it-utrymmen

Med en rutin avses någon form av bestämmelse/regel/instruktion eller liknande som beskriver handlande i en specifik situation eller specifikt tillstånd. En rutin kan också beskriva arbete med ett specifikt objekt. En rutin kan vara muntlig men bör nedtecknas till en skriftlig instruktion, bestämmelse, regel eller liknande.

Följande rutiner bör skapas av en organisation som ansvarar för den fysiska informationssäkerheten i it-utrymmen:

- **Rutiner för tillträde**
  Ska beskriva hur tillträde söks, godkänns och implementeras. Vem eller vilka som ska ha tillträde ska framgå. Var noggrann med att skilja på egen personal och extern personal från exempelvis serviceorganisationer.
- **Rutiner och förvaring av passerkort, taggar och nycklar**
  Rutinen ska beskriva hur medarbetare ska förvara enheter som ska användas vid tillträde. Denna rutin kan även innehålla reglering för externa parter om passagemöjligheter finns.
- **Rutiner vid byggnation, underhåll och service**
  Ska beskriva hur arbeten som är av karaktären byggnation, underhåll och service får utföras i it-utrymmen. Exempel på arbeten kan vara reparation av kylaggregat, elinstallationer, heta arbeten och borrning. Det är viktigt att alla typer av arbeten i it-utrymmen som potentiellt kan skada utrustning och datamedia ges särskild uppmärksamhet.

> En av de vanligaste orsakerna till incidenter i it-utrymmen är att reparatörer eller installatörer är oaktsamma. Många personer i denna yrkeskategori vet inte hur man ska agera i ett it-utrymme. Incidenter som omfattande strömavbrott orsakade av att elmaskiner ansluts i UPS-uttag eller att man borrar så damm ryker in i utrustning som kostar > 1 miljon kronor är bara några exempel på verkliga händelser.

- **Rutiner för installation, anslutningar och montage**
  Ska beskriva hur installation av el, data och utrustningar utförs. Dessutom ska det beskrivas hur it-utrustning ska monteras och anslutas inne i it-utrymmet. Exempel kan vara hur utrustning ska vändas, hur el ansluts, hur elgrupper fördelas, färger på kablar, hur datanät ansluts och liknande uppgifter.
- **Rutiner för märkning**
  Ska beskriva hur uttag (el och data) samt utrustningar ska märkas. Det finns normer för hur märkning ska ske, men överväg alltid att komplettera med strukturer som gör det enkelt för personalen att finna och spåra.
- **Rutiner för städning**
  Städning i it-utrymmen ska utföras av utbildad personal. Rutinerna för städning ska beskriva vem som ska städa, hur städningen ska utföras, vilka typer av maskiner som får användas samt med vilken frekvens detta ska ske.

Det är en god idé att använda personal som är utbildad för städning av utrymmen som innehåller känslig elektronisk utrustning. Det är tyvärr vanligt att incidenter sker i it-utrymmen då outbildad personal används. Städning i it-utrymmen ska i huvudsak ske via att ytor och utrustning torkas av med fuktad trasa för att undvika att statisk elektricitet bildas.

- **Rutiner för prov och övningar (t.ex. katastrofövningar)**
  Organisationen ska utveckla rutiner för prov och övningar knutna till olika händelser i verksamhetens it-utrymmen. Dessa typer av rutiner är vitala för att konsekvenserna av incidenter ska kunna minimeras. Övningar bör utföras löpande.
- **Rutiner för brandsläckning**
  I händelse av en brand ska det finnas rutiner som beskriver hur personalen ska agera. Detta kan exempelvis inkludera hur och när man ska försöka släcka en brand, hur handbrandsläckare ska användas eller hur personalen ska agera om man har automatiska släckningssystem.
- **Fotoförbud**
  Rutinen ska beskriva om fotoförbud råder samt omfattningen av ett sådant, och om exempelvis speciella tillstånd krävs för att fotografera. Har en verksamhet ställverk för kraftmatning inne i eller nära it-utrymmen kan dessa vara utrustade med ljusbågsvakter. En ljusbågsvakt är en säkerhetsutrustning som bryter strömmen i händelse av en kortslutning (som i ett ställverk skapar en ljusbåge/blixt). Problemet är att ljusbågsvakter är känsliga för fotoblixtar och det kan alltså räcka att ta en bild med blixt för att bryta strömmen till en datorhall. Fotoförbud ska därför alltid respekteras.
- **ESD rutiner (ESD-policy)**
  ESD (ElectroStatic Discharge) eller urladdning av statisk elektricitet kan vara ett stort problem i it-utrymmen och kan skada känslig elektronisk utrustning. Rutinen ska därför beskriva hur riskerna för urladdning ska minskas. Detta kan inkludera hur personal alltid ska bära viss utrustning, gå över vissa ytor som minskar uppbyggnad av statisk elektricitet eller liknande regler.
- **Rutiner för förvaring av skräp**
  Ska beskriva att skräp, papper, kartonger och liknande inte ska förvaras i ett it-utrymme. Inget material som är lättantändligt ska förvaras i ett it-utrymme. Uppackning av it-utrustning ska alltid ske utanför it-utrymmet och alla kartonger etc. ska avlägsnas. Rutinen ska också beskriva att soptunnor, papperskorgar och liknande inte ska förvaras i ett it-utrymme.
- **Rutiner för förvaring av brandfarligt material**
  Denna rutin ska beskriva att alla brandfarliga eller explosiva material eller ämnen inte ska förvaras inne i eller i närheten av ett it-utrymme. Rutinen bör även innehålla regler som förbjuder användning av möbler av brännbart material i it-utrymmen.
- **Mat och vätskor (t.ex. te och kaffe)**
  Personal vill gärna ta med sig mat och vätskor som läskedrycker, te och kaffe in i it-utrymmen. Rutiner bör beskriva att detta inte är tillåtet eftersom incidenter kan ske genom att någon är oaktsam.

- **Rutiner för funktionsprov**
  Följande rutiner ska skapas för funktionsprov av skyddsmekanismer i en verksamhets it-utrymmen. Generellt ska dessa rutiner utföras återkommande med jämna intervall:
  - **Reservkraft**
    Ska beskriva hur reservkraftsaggregat provas och med vilken frekvens. Bör inkludera delvisa prov där aggregaten enskilt provas. Minst en gång per kvartal bör hela funktionskedjan provas, då inkommande elmatning bryts och simulerar ett strömavbrott.
  - **UPS**
    Ska beskriva hur avbrottsfri kraft provas och med vilken frekvens. Beroende av prov av reservkraft ska beskrivas. Bör också innehålla kontroller av batterier anslutna till eller i UPS-enheter. Rutinen ska också beskriva hur kontroller av UPS kapacitet sker så att utrustningar inte överbelastas.
  - **Kyla, reservkyla och nödkyla**
    Dessa rutiner ska innehålla beskrivningar av kontroller för kylaggregat. Kontroller av kapacitet ska ske så att anläggningen inte överbelastas. Rutiner ska också beskriva hur en verksamhet provar sina reservkylaggregat eller sin nödkyla. Dessa funktioner bör provas minst en gång per halvår.
  - **Brandlarm**
    Rutiner ska beskriva hur brandlarm provas och i vilken omfattning. Rökprov med test av branddetektorer bör ske minst en gång per år.
  - **Automatiska släckanläggningar**
    Rutiner ska beskriva hur automatiska släckanläggningar provas och i vilken omfattning. Rutinen ska exempelvis även inkludera kontroller av släckmedel via avläsning av tryck i gasflaskor.
  - **Handbrandsläckare**
    Ska beskriva kontroll av korrekt funktion och rutiner för påfyllning av släckmedel. Eftersom handbrandsläckare i och nära it-utrymmen ofta befinner sig i egna säkerhetszoner missas det ofta att kontrollera dessa handbrandsläckare i det systematiska brandskyddsarbetet för den övriga verksamheten.
  - **Inbrottslarm**
    Ska beskriva prov och kontroller av inbrottslarm. Överväg att genomföra prov av hela funktionskedjan till bevakningsorganisationen minst en gång vartannat år.
  - **Fuktlarm (vattenlarm)**
    Ska beskriva prov och kontroller av fuktlarm. Kontroller bör ske minst en gång per år.
  - **Temperaturlarm**
    Ska beskriva kontroller och prov av temperaturlarm. Kontroller bör ske minst en gång per år.
  - **Rutiner för service**
    Dessa rutiner ska beskriva hur verksamheten ämnar upprätthålla funktionen i samtliga tekniska säkerhetsskydd. Vanligen tecknas serviceavtal med interna eller externa organisationer för denna uppgift. Vidare ska även rutinen inkludera hur dessa serviceåtaganden kontrolleras. Dessa kontroller kan exempel-

vis genomföras genom att falska larm skapas och verksamheten kontrollerar då hur lång tid serviceorganisationen tar på sig för att agera. Denna typ av kontroller bör inkluderas i serviceavtal.

– **Rutiner för extern granskning (audit)**
Ska beskriva hur en verksamhet genomför externa granskningar av sin fysiska informationssäkerhet i it-utrymmen. Denna typ av granskning bör genomföras löpande, åtminstone vartannat år, av extern opartisk expertis.

# Bilaga 3

# Bilaga 3 – Förvaring av säkerhetskopior

Alla ansvarsfulla verksamheter ser till att säkerhetskopiera vital information så att denna kan återskapas vid en incident. Säkerhetskopior tas i dag vanligtvis ut på CD-media eller databand, men det blir vanligare med elektroniska säkerhetskopior på hårddisk. Databand tar man normalt ur sin bandstation eller bandrobot och förvarar på en plats som är skild från it-utrymmet, vanligtvis ett säkerhetsskåp. Ytterligare en vanlig lösning är att placera säkerhetskopieringsutrustningen (t.ex. bandrobot) i ett eget utrymme, vilket då likställs med förvaring i säkerhetsskåp[21].

Men görs säkerhetskopior endast till hårddisk är situationen annorlunda eftersom dessa vanligen är fast monterade i kabinett eller stativ och inte är lika flyttbara. Därför har många verksamheter sina säkerhetskopior i samma it-utrymme som it-utrustningen. Denna situation är tyvärr vanlig idag och kan utgöra en stor risk för många verksamheter.

> Förvara aldrig säkerhetskopior i samma utrymme som it-utrustningen. Om en incident sker i eller utanför it-utrymmet riskerar man att helt förlora stora mängder vital information.

*Separation*

Flera verksamheter har dock på senare tid uppmärksammat denna situation och valt att flytta elektroniska säkerhetskopior till ett separat utrymme. Placeringen av elektroniska säkerhetskopior ska inte vara i närheten av det ordinarie it-utrymmet eftersom en incident då kan slå ut båda dessa utrymmen. Observera också att om elektronisk lagring flyttas ut i ett separat utrymme så bör dessa lokaler följa samma krav på fysiska skydd som gäller för övriga it-utrymmen.

> Kontrollera att de skåp som används för att förvara säkerhetskopior är avsedda för ändamålet. Det är vanligt att verksamheter förvarar exempelvis databand med säkerhetskopior i skåp som är anpassade för pappersförvaring. Vid en brand riskerar databanden att förstöras.

*Inbrottstest och inbrottsklassning*

För att tillgrepp av säkerhetskopior inte ska kunna ske behöver också en förvaring vara försedd med en inbrottsklass. Innan ett skåp får en säkerhetsklassning så måste det genomgå ett övervakat inbrottstest. I Sverige är det Stöldskyddsföreningen tillsammans med Rikspolisstyrelsen som genomför inbrottstester. Externa

21. Riksarkivet har krav på att myndigheter ska framställa säkerhetskopior av samtliga allmänna handlingar samt att säkerhetskopiorna ska förvaras geografiskt åtskilt från de kopierade elektroniska handlingarna (RA-FS 2009:1, 6 kap. 5 §).

kravställare som myndigheter och försäkringsbolag ställer ofta krav på att förvaringen av skyddsvärda resurser ska vara inbrottsklassad. I Sverige är de vanligaste inbrottsklasserna för förvaring följande:

– **SS 3492**
Säkerhetsskåp är numera den enda förekommande klassningen i SS 3492. Skåpen är tillverkade i 4 mm stålplåt och uppfyller vissa krav som ställs på lås och regelsystem. SS 3492 ger möjlighet att försäkra vissa värden och är också minimikrav för viss förvaring, t.ex. av vapen. Certifikat utfärdas av DNV (Det Norske Veritas) eller Svensk Brand & Säkerhetscertifiering AB (SBSC).

– **SS 3493**
Motsvande tester som säkerhetsskåp i SS 3492, men skåpen är dessutom brandklassade.

– **EN 1143-1**
EN 1143-1 är en europeisk standard för inbrottsklassning av värdeskåp som kan kombineras med ett explosionstest. En gradering används för att skilja på olika säkerhetsnivåer. Klassningen börjar på Grade 0 och den högsta klassningen i Sverige är Grade VI EX, där EX anger att skåpet är explosionstestat.

– **EN 1143-2**
Denna norm är jämförbar med den föregående men gäller för enklare typer av skåp som deponeringsskåp.

– **EN 14450**
Europeisk standard som i säkerhetsnivå kan jämföras med den äldre normen Stöldskyddsskåp 1 och 2, klassningen anges S1 respektive S2. Försäkringsbolag godkänner ingen värdeförvaring i dessa typer av skåp.

– **Övriga**
Det finns övriga skåp med andra klassningar som är godkända för värdeförvaring. SS 3150 är ett exempel där skåpets skyddsnivå redovisas i ett poängsystem som anges i intervall. Högre poäng ska motsvara högre säkerhet. Riktigt gamla värdeskåp har klassningen V1, V2, V2S eller V3. Samtliga av dessa skåptyper förekommer på begagnatmarknaden och är godkända för förvaring av värden från 10 000 kronor upp till miljonbelopp beroende på klassningen.

*Brandtest och brandklasser*

I Sverige är följande metoder och klassningar vanligt förekommande. Proven och klassningen är relevanta för test av förvaring och utförs i en ugn för att efterlikna ett brandförlopp:

– **NT Fire 017**
NT Fire 017 är en nordisk standard som innefattar regelbunden produktionskontroll och krav på återtestning. Förvaring certifieras i 60P, 90P eller 120P (för papper) alternativt 60 DIS eller 120 DIS (för datamedia). Talen anger antal minuter i ugnen. Tester utförs i Sverige av Sveriges Provnings- och Forskningsinstitut (SP) som också utfärdar certifikat.

– **SS-EN 1047-1**
Detta är en europanorm som även inkluderar fall- och chocktest där mätning av innetemperatur fortsätter under avsvalningsfasen. Årlig produktionskontroll sker. Skåp certifieras i S 60P eller S 120P (för papper), alternativt S 60 DIS eller S 120 DIS (för datamedia). Testet kan utföras på auktoriserade institut, vilka finns i flera länder i Europa, och certifikaten utfärdas av European Security Certification Board Security Systems (ECB.S).

- **SS-EN 1047-2**
  Del två av denna testmetod är anpassad för hela it-utrymmen och begränsas inte bara till en enskild skåpförvaring. Mer om denna metod och klassningar återfinns i kapitel 2.4 om brandskydd för it-utrymmen.
- **UL (Underwriters Laboratories)**
  UL är ett amerikanskt brandtest som kan inkludera fall- och chocktest om detta begärs. Årlig produktionskontroll kan genomföras. Skåp certifieras i 1H eller 2H som anger en eller två timmars test. Test sker både för papper och datamedia. Institut SOMO, auktoriserade av UL, hanterar testerna och UL utfärdar certifikat.
- **JIS**
  JIS är ett japanskt test där skåp certifieras i 60P eller 120P (för papper). Finns endast i P-test, dvs. test för skydd av papper.
- **KSG-4500**
  KSG-4500 är ett koreanskt brandtest och skåp certifieras i 60P eller 120P (för papper). Finns endast i P-test, dvs. test för skydd av papper.

I Sverige är de vanligast förekommande certifieringarna NT Fire 017 och SS-EN 1047-1. De förekommer oftast som krav vid upphandlingar från offentlig sektor och större företag med högt säkerhetstänkande. UL-testet är också på väg att bli mer vanligt förekommande.

*Rekommendationer*
Förvara alltid datamedia i skåp som är brandklassade för en sådan förvaring, exempelvis S60 DIS eller S120 DIS. Förvaringen ska också vara inbrottsklassad, exempelvis enligt SS 3492. Använder man ett separerat utrymme för sin datamedialagring ska utrymmet lämpligen klassas som om det vore ett skåp. SS/EN1047-2 är då en lämplig klassning.

# Bilaga 4

# Bilaga 4 – Exempelberäkning av kyleffektsbehov

Ytterligare ett sätt för att få fram kyleffektsbehovet är att beräkna utifrån märkeffekten på alla it-utrustningar i utrymmet. Detta kan vara tidsödande och tenderar också ge en något felaktig bild över behovet eftersom inga it-utrustningar förbrukar ”märkeffekten” konstant hela tiden.

Det finns mer avancerade former av beräkning för kyleffekter som används av expertis inom området. Nedan presenteras en modell (BTU[22]-beräkning), som visserligen är relativt ovanlig men som ändå kan vara till hjälp för att få fram kyleffektsbehovet för ett it-utrymme. En förenklad beräkningsmodell kan uppskatta effektbehovet, men konsultera alltid expertis för en mer detaljerad och korrekt beräkning.

Beräkningen baseras på den värmeeffekt som alstras från utrustning, lokalens yta, öppningar och fönster, antalet personer i lokalen samt belysning. En kilowatt värmeffekt (1 kW) motsvaras av 3412 BTU.

A: Rumsytans BTU = längd (m) * bredd (m) * 337

B: Fönster (södervänt) BTU = höjd (m) * bredd (m) * 870 (per fönster)

C: Fönster (norrvänt) BTU = höjd (m) * bredd (m) * 165 (per fönster)

D: Personers BTU = antalet personer i lokalen * 400

E: Utrustningens BTU[23] = (summan av effektmärkning (Watt) på alla it-utrustningar) * 3,5

F: Belysningens BTU = (totala belysningseffekten i Watt) * 4,25

G: Utrymmets totala värmebelastning = summan av (A-F)

Totalt kyleffektsbehov (kilowatt) = G/3,412

En uppenbar nackdel med denna metod är att den anger det momenta behovet och tar inte hänsyn till utbyggnad. Förändra därför enhet E (utrustningens behov) att motsvara ett framtida behov.

22. BTU (British Thermal Unit)
23. Hos vissa tillverkare anges utrustningars värmealstrande effekt direkt i enheten BTU

# Bilaga 5

# Bilaga 5 – Exempelberäkning för UPS-kapacitet

Volt Ampere och Watt beskriver olika typer av effekt. Förhållandet mellan dessa två enheter styrs av en effektfaktor som varierar mellan 0 och 1 enligt förhållandet Watt = effektfaktorn * VA. För modernare it-utrustning är effektfaktorn 0,9 medan äldre utrustningar har lägre effektfaktor (0,6–0,7).

Exempel: Beräkna kapacitetsbehovet hos en UPS i ett it-utrymme med 30 stycken moderna servrar som vardera är märkta 400 Watt:

*Kapacitetsbehov (VA) = (30*400)/0,9 = 13333 VA.*

*En UPS-enhet med kapaciteten 13 500 VA (13,5 kVA) är lämplig kapacitet.*

*I våra it-utrymmen sker det ständigt förändringar och man ska därför aldrig välja att lasta en UPS till dess maximala kapacitet eftersom skalbarheten och flexibilitet kommer att bli lidande. En typisk rekommendation är att aldrig belasta en UPS högre än maximalt 75–80 %. En mer praktisk nivå av maximal last är kring 60–65 %, om man har behov för utbyggnad inom de närmaste åren.*

*Rekommendationen till lämplig kapacitet förändras då i exemplet med hänsyn taget till maximal belastning till: 13,5 kVA då till: 13,5/0,65 = 20,8 kVA. Anvrundat är alltså en effekt hos UPS-enheten på 21 kVA lämplig.*

Ett samarbete mellan


Myndigheten för
samhällsskydd
och beredskap

Riksarkivet

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad  Tel 0771-240 240  www.msb.se
Publ.nr MSB629 - december 2013  ISBN 978-91-7383-401-8