

HANDBOK

SÄKERHET VID ENERGIFÖRETAG

FÖRORD

En väl fungerande energiförsörjning är en nödvändig förutsättning för ett fungerande samhälle.

Företag verksamma inom energiförsörjningen utsätts varje dag för olika slags angrepp, bl. a. i form av inbrott, skadegörelse eller IT-angrepp. Under senare år har också organiserad brottslighet ökat vilket kan påverka arbetet i företagen men också drabba enskilda medarbetare.

Under 1999 togs det fram en säkerhetshandbok för elförsörjningen. Avsikten var att boken skulle vara ett verksamt hjälpmedel för hela energiförsörjningen.

En arbetsgrupp med representanter från Svensk Energi har tillsammans med Svenska Kraftnät arbetat med att ta fram en reviderad version av handboken. Energigas Sverige och Svensk Fjärrvärme har stött arbetet och lämnat värdefulla bidrag. Resultatet av arbetet är denna omarbetade säkerhetshandbok. Syftet är att alla företag verksamma inom energiförsörjningen ska kunna använda handboken som ett hjälpmedel i sitt säkerhetsarbete.

Samhället är idag mer beroende än tidigare av ett väl fungerande informationssystem. Samtidigt har störningar i normal drift fått allt större inverkan på det normala arbetet. Informationssäkerhet har därför fått en central roll i handboken.

Målgruppen för handboken är säkerhetschefer, säkerhetssamordnare eller säkerhetsskyddschefer i enlighet med kraven i säkerhetsskyddslagen. I handboken används dock genomgående begreppet säkerhetschef.

Vi vill tacka alla som deltagit i arbetsgrupp, referensgrupp, styrgrupp och övriga som lämnat värdefulla bidrag för att handboken ska bli ett användbart hjälpmedel i säkerhetsarbetet.

SID	INNEHÅLL
4	1. SAMMANFATTNING
5	2. ANSVAR OCH SAMVERKAN
8	3. HOT, RISKER OCH FÖRMÅGA
11	4. PERSONALSÄKERHET
14	5. INFORMATIONSSÄKERHET
20	6. ANLÄGGNINGSSÄKERHET
26	7. KRISBEREDSKAP
29	8. SAMHÄLLSVIKTIG VERKSAMHET
34	BILAGOR
35	BILAGA 1 - LAGAR OCH FÖRORDNINGAR
40	BILAGA 2 - BEFATTNINGSBESKRIVNING FÖR FÖRETAGETS SÄKERHETSFUNCTION
42	BILAGA 3 - EXEMPEL PÅ SKYDDSVÄRDA UPPGIFTER
44	BILAGA 4 - TYSTNADSFÖRBINDELSE
45	BILAGA 5 - SEKRETESS- OCH SÄKERHETSAVTAL
49	BILAGA 6 - PERSONALHANTERING ANSTÄLLDA
51	BILAGA 7 - PERSONALHANTERING ÖVRIG PERSONAL
53	BILAGA 8 - ÅTGÄRDER VID BOMBHOT
55	BILAGA 9 - CHECKLISTA INFORMATIONSSÄKERHET VID HANTERING AV IT-SYSTEM
67	BILAGA 10 - AWWIKELSE- OCH HÄNDELSEHANTERING

1. SAMMANFATTNING

BAKGRUND

Företag i energibranschen råkar varje år ut för skadegörelse, inbrott, stölder och andra kriminella handlingar. Virus i datorer eller andra störningar som orsakas av utomstående IT-system skapar stora problem. Då och då inträffar också allvarligare händelser såsom större bedrägerier, bränder och sabotage i anläggningar. I takt med allt hårdare konkurrens ökar också intresset av att ta del av information från konkurrenter och därmed ökar också risken att drabbas av informationsstöld.

Inom energibranschen har ordet säkerhet flera betydelser. Den typ av säkerhet som behandlas i denna handbok avser i första hand skydd mot våld, stöld, sabotage och ekonomisk brottslighet samt säkerhetsskydd enligt säkerhetsskyddslagsstiftningen. Det går dock inte att dra någon knivskarp gräns mellan olika säkerhetsområden vilket innebär att även en del angränsande områden behandlas i denna handbok.

Energiföretag har att följa ett flertal lagar, förordningar och föreskrifter i syfte att vidta åtgärder för att skydda personal, egendom och säkra landets energiförsörjning. Ett urval av de viktigaste lagarna redovisas i bilaga.

Med energiföretag avses i denna handbok bolag, företag, föreningar och förvaltningar som är verksamma inom produktion, distribution och försäljning av el, värme och gas med tillhörande tjänste-, entreprenad- och serviceverksamheter.

SYFTE

Syftet med handboken är att bland annat stödja energiföretagen i arbetet med riskanalys, värdering av hot, upphandlingar, införande av bevakningsteknik, framtagande av egna riktlinjer samt genomförande av utbildning.

Eftersom handboken är skriven för att passa olika personalkategorier kan innehåll och detaljnivå i handbokens kapitel skifta.

INNEHÅLL

Handboken är skriven för att kunna läsas i ett sammanhang, men också för att fungera som en uppslagsbok. Texten får kopieras och spridas. En kort innehållsbeskrivning av bokens kapitel:

Ansvar och samverkan – beskriver aspekter på säkerhetsansvaret inom företaget, men behandlar också samverkansparter internt och externt.

Hot, risker och förmåga – tar kortfattat upp risker och hot mot företag och betydelsen av att följa upp avvikelser och incidenter. Ett utvecklat riskhanteringsarbete inom företaget skapar förutsättningar att undvika risker och kostnader.

Personalsäkerhet – omfattar de säkerhetsåtgärder som är knutna till företagets medarbetare. I tillhörande bilagor finns konkreta checklistor och mallar.

Informationssäkerhet – behandlar information i traditionell form på papper, kartor och bilder samt i elektronisk form i databaser, e-post och telekommunikation.

Anläggningssäkerhet – ger bland annat råd kring ett väl avvägt anläggningsskydd.

Krisberedskap – ger kortfattat råd för företagets krisberedskap och krishantering. En utveckling av kapitlet planeras i annan handledning och då med fokus på samhällets krisberedskap.

Samhällsviktig verksamhet – beskriver samhällsviktig verksamhet, skyddsobjekt och säkerhetsskydd.

2. ANSVAR OCH SAMVERKAN

ANSVARSFÖRDELNING OCH POLICY

Ansvar för säkerhet ligger alltid hos dem som har huvudansvaret för ett företags verksamhet, det vill säga dess styrelse och VD. Den som samordnar säkerhetsarbetet kallas normalt säkerhetschef men olika benämningar kan finnas, exempelvis säkerhetsstrateg, säkerhetssamordnare och säkerhetscontroller. I denna publikation benämns funktionen säkerhetschef. Säkerhetschefen bör ha en tydlig dubbelriktad kommunikation med företagets VD, ledningsgrupp, chefer och övrig personal. För de företag som har verksamhet av betydelse för rikets säkerhet utses en säkerhets-skyddschef, se kapitel 8.

Målsättningen med säkerhetsarbetet bör finnas i en policy som fastställs av företagets styrelse och VD. Punktsatserna nedan kan helt eller delvis utgöra en grund i de flesta företags säkerhetspolicy:

- En effektiv riskhantering inom ett energiföretag är en väsentlig faktor för bibehållande av företagets konkurrensposition på marknaden samt trovärdigheten gentemot företagets kunder.
- Att förvalta, utveckla och som ett led häri skydda företagets tillgångar är ytterst en skyldighet och ett ansvar för den verkställande ledningen. Processen i organisationen bör ske i samverkan med samtliga medarbetare.
- Skydda de anställda som är företagets viktigaste tillgång. Samarbeta med de anställda – då skyddas också företaget.
- Riskhantering syftar till att förebygga och begränsa skador på företagets tillgångar och på miljön. Medarbetare, kunskap och information är viktiga tillgångar för företaget.
- All riskhantering samordnas och grundas på en total riskanalys. Detta som ett led i företagets riskmanagementarbete, vilket kontinuerligt ska revideras. Verksamheten ska inriktas och planeras med utgångspunkt från genomförda riskanalyser.

Utifrån denna grundsyn kan varje företag utforma egna konkreta mål och delmål för sitt säkerhetsarbete.

Ansvar för att värdera risker och vidta rimliga förebyggande och skadebegränsande åtgärder vilar i de flesta svenska företag på styrelse, VD och resultatansvariga chefer. En säkerhetschef fungerar i regel som stabsresurs och ges en samordnande, rådgivande och stödjande roll gällande risker och åtgärder för att hantera dessa. En säkerhetschefs ansvarsområde kan även omfatta den totala riskhanteringen i företaget (risk management), försäkringar, brandskydd, IT-säkerhet, missbruksfrågor, katastrofberedskap, miljö, arbetsmiljö och kvalitet.

Det uppdrag som en säkerhetschef har från VD bör dokumenteras i en befattningsbeskrivning, ett delegeringsdokument eller en särskild instruktion där även samråds- och rapporteringsvägar samt avgränsning mot andra närliggande områden anges. Exempel redovisas i bilaga.

En säkerhetschef ska verka för att riskmedvetande finns hos alla i företaget och att säkerhetskänslighet finns inarbetad i alla processer. Det underlättar väsentligt för verksamhetsansvariga om styrdokument, instruktioner, uppföljningssystem m. m. är samordnade.

SYSTEMATISKT SÄKERHETSARBETE

Säkerhetsarbetet (security) ska bedrivas systematiskt för att i möjligaste mån förhindra inbrott, stöld, svinn, bedrägeri, hot, rån, sabotage, spionage och intrång i IT-system med mera. Att regelverk följs och att tekniska system fungerar och används bör följas upp. Uppföljning är därför en viktig del av säkerhetsarbetet. För att få bra beslutsunderlag gällande säkerhetshöjande åtgärder är det värdefullt med en fungerande intern rapportering av avvikelser, incidenter, risker och skador.

Motsvarande systematik kan användas vid annat säkerhetsarbete (safety).

I bilaga 10 finns exempel på avvikelse- och händelsehantering.

Systematiskt säkerhetsarbete pågår ständigt och utvecklas – exempelvis genom att arbetet sker i en process där riskanalysen har en central roll. Säkerhetschefen är den som ska se till att processen fungerar.

Exempel på process:

- 1. Riskbild.** Vad hotar verksamheten? Inventera externa och interna hot samt analysera dessa.
- 2. Planera/organisera** för att eliminera/möta hoten genom att exempelvis se till att sabotagekänsliga platser övervakas och förhindra ensamarbete då hotsituation kan förväntas. Allt som planeras ska även finansieras.
- 3. Genomför** de planerade åtgärderna.
- 4. Utvärdera och följ upp** om åtgärderna fått önskad effekt.
- 5. Förbättra och utveckla** med beaktande av det som kommit fram vid utvärdering.

UPPFÖLJNING OCH REVISION

Periodisk uppföljning och revision av säkerhetsarbete ska planeras och genomföras. Det är ett bra styrmedel och skapar goda förutsättningar för att förbättra och rätta till fel i regelverk och rutiner. En policy för hur detta ska gå till bör tas fram. Viktigt är att periodiciteten i antalet uppföljningar avvägs så att det inte uppfattas som om de genomförs alltför tätt. Risker är då att de anställda kan uppfatta detta som brist på förtroende vilket kan påverka organisationen negativt.

UTBILDNING

En säkerhetschef ska vara rätt utbildad för att kunna agera inom de ansvarsområden som befattningen innebär. Det finns ett flertal olika utbildningar att tillgå inklusive en certifiering för säkerhetschefer som genomförs av Svensk Brand- och Säkerhetscertifiering. Det är en så kallad tredjeparts-certifiering som refererar till den internationella standarden SS-EN ISO/IEC 17024:2003. Förutom lämplig teoretisk utbildning är praktisk erfarenhet av stor betydelse.

SAMVERKAN

Samverkansområden för säkerhetschef inom företaget kan till exempel vara en säkerhetskommitté inom företagsgruppen eller inom en viss kontorsgemenskap. I större företag kan resurser ofta samlas i en stab för att exempelvis stödja en hel koncern.

EXTERN SAMVERKAN

Företagsledning och säkerhetschef bör eftersträva ett bra samarbete med myndigheter, organisationer och företag. Ett fungerande nätverk för säkerhetssamverkan är en förutsättning för ett väl fungerande säkerhetsskydd. Kännedom om samverkande myndigheters organisation, uppgifter och resurser är nödvändig.

Exempel på samverkande myndigheter, organisationer och företag:

- > Bevakningsföretag
- > Brottsförebyggande rådet – www.bra.se
- > Energibranschens resurscentrum i alkohol- och drogfrågor, EBRID – www.ebrid.org
- > Energigas Sverige – www.energigas.se
- > Energimarknadsinspektionen – www.ei.se
- > Företagets externa revisionsföretag
- > Försvarsmakten – www.mil.se
- > Försäkringsbolag
- > Kommunerna
- > Larminstallatörer
- > Länsstyrelserna – www.lansstyrelsen.se/1st
- > Myndigheten för samhällsskydd och beredskap, MSB – www.msb.se
- > Näringslivets säkerhetsdelegation, NSD – www.svensktnaringsliv.se/nsd
- > Polisen – www.polisen.se
- > Post och Telestyrelsen, PTS – www.pts.se
- > Räddningstjänst
- > SOS Alarm – www.sosalarm.se
- > Statens energimyndighet – www.energimyndigheten.se
- > Strålsäkerhetsmyndigheten – www.ssm.se
- > Svensk Energi (Ag Säkerhet och beredskap, EBITS) – www.svenskenergi.se
- > Svensk Fjärrvärme AB – www.svenskfjarrvarme.se
- > Svenska Brandskyddsföreningen – www.brandskyddsforeningen.se
- > Svenska Kraftnät, SvK – www.svk.se
- > Svenska Stöldskyddsföreningen – www.stoldskyddsforeningen.se
- > Sveriges Kommuner och Landsting – www.skl.se
- > Säkerhetskonsulter
- > Säkerhetspolisen, SÄPO – www.sakerhetspolisen.se

Dessutom finns det flera branschöverskridande nätverk, allt ifrån lokala kommunala nätverk till nationella och internationella nätverk.

3. HOT, RISKER OCH FÖRMÅGA

HOT OCH RISKER MOT FÖRETAGET

Utvecklingen i såväl Sverige som i vår omvärld medför att förutsättningarna att bedriva verksamhet hela tiden förändras. Varje chef måste därför kontinuerligt ta ställning till hot och risker inom sitt ansvarsområde. En kontinuerlig uppföljning av händelser som inträffat både inom och utom företaget ökar möjligheten att vidta rätt åtgärd vid rätt tidpunkt. Det är även viktigt att följa vad som händer lokalt och regionalt, exempelvis i form av missnöjes- och opinionsyttringar eller politiska händelser. Det är också väsentligt att kunskaper om existerande hot och möjliga skyddsåtgärder sprids inom företaget.

För detaljer kring begreppet riskhantering samt dess innehåll hänvisas till Fermas (Federation of European Risk Management Associations) **Standard för risk management** samt till föreningen SWERMA (Swedish Risk Management Association).

Syftet med att identifiera hot och risker är att:

- > öka företagets kunskap och medvetenhet i syfte att stärka företagets förmåga och roll i samhällets infrastruktur,
- > identifiera orsaker och villkor som kan leda till att en händelse utvecklas till en allvarlig situation för företaget eller för samhället och
- > upptäcka kritiska beroendeförhållanden inom och mellan verksamheter.

Det är viktigt att en analys av säkerhetsrisker görs förutsättningslöst. Risker hör till stor del samman med den verksamhet som respektive företag bedriver. Nedan följer några generella exempel på säkerhetsrisker:

- > ekonomisk brottslighet,
- > grov organiserad brottslighet,
- > informationsförlust (se bilaga),
- > stöld, skadegörelse och sabotage,
- > intern brottslighet,
- > fysiska och psykiska skador på personal (exempelvis vid hot och våld),
- > störning eller utslagning av samhällsviktiga funktioner,
- > energistöld (olovlig kraftavledning) samt
- > andra risker.

SKYDDSVÄRDA DELAR

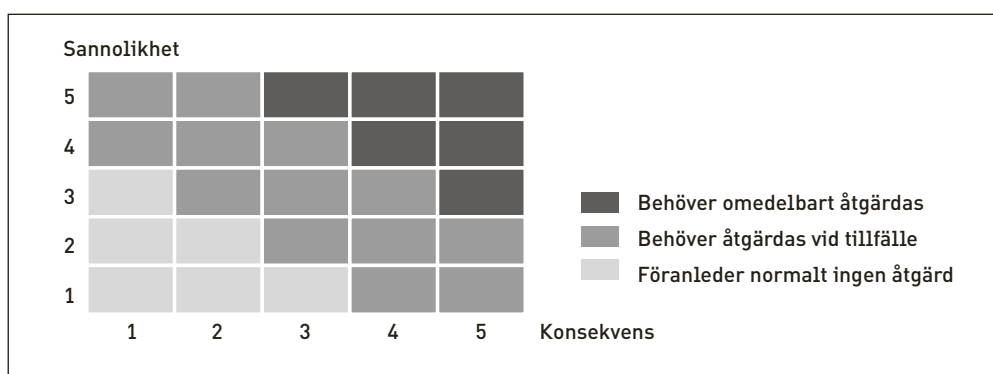
Företaget bör, innan riskarbetet startar, göra en inventering och genomgång av vad som är företagets viktigaste tillgångar och mest skyddsvärda delar. De kan vara både materiella eller immateriella tillgångar. I arbetet bör också ingå att prioritera vilka delar som riskarbetet huvudsakligen ska inriktas på. Riskidentifiering, analys och åtgärdsförslag kan med fördel brytas ner i mindre delar för att underlätta investeringar, utbildning eller försäkringsåtgärder.

RISKANALYS

Riskanalys innebär en systematisk identifiering och värdering av risker utifrån hur sannolikt det är att något inträffar och vilka konsekvenser detta i så fall skulle medföra. Detta leder sammantaget fram till en bedömd risknivå. När man inleder arbetet med en riskanalys är det viktigt att man klargör syftet med analysen. Vidare behöver man göra en avgränsning, det vill säga fastställa vad analysen ska behandla och i vilket skede den ska genomföras (exempelvis vid nybyggnation eller på befintlig verksamhet). Sedan behöver man välja typ av analysmetod samt göra en kostnads- och nyttobedömning.

ANALYSMETOD

Det finns flera olika typer av analysmetoder. I denna handbok beskriver vi den vanligaste metoden som brukar kallas **Kvalitativ analysmetod (Grovanalys)**. Denna analysmetod används för att identifiera riskkällor och/eller riskfyllda situationer.



RISKIDENTIFIERING

Att identifiera vilka risker som är kopplade till den verksamhet som bedrivs är grunden för all riskhantering, exempelvis:

- > händelser som inträffat inom egen eller liknande verksamhet,
- > uppenbara händelser med tanke på verksamhetens karaktär samt
- > potentiella händelser eller kombinationer av händelser som tidigare ej inträffat.

RISKVÄRDERING

Genom att grovt skatta sannolikheten och konsekvensen för var och en av riskerna kan man rangordna riskerna med hänsyn till hur allvarliga de är och identifiera de som behöver analyseras i detalj. Den formel som generellt brukar användas är:

$$\text{sannolikhet} \times \text{konsekvens} = \text{riskvärde}$$

RISKHANTERING

Avgör vilka risker som kan accepteras (kalkylerade risker) och vilka som inte kan accepteras och som därmed måste begränsas genom förebyggande och/eller skadebegränsande åtgärder.

ÅTGÄRDSPLAN

Företaget bör upprätta en åtgärdsplan för att hantera och åtgärda de risker som framkommit vid riskanalysarbetet. Åtgärdsplanen är ett verktyg för att prioritera vilka risker som ska hanteras på både kort och lång sikt. En åtgärdsplan sammanfattar och presenterar på ett lättillgängligt sätt riskerna och rangordnar dessa efter hur allvarliga de är. En tydlig ansvarsfördelning bidrar till att klargöra vem som "äger" risken och att den ägnas tillräcklig uppmärksamhet från ledningens sida.

MÖJLIGHETER ATT MÖTA HOT (FÖRMÅGEBEDÖMNING)

Vilken förmåga en organisation, ett bolag eller en anläggning har att skydda sig, är något som också måste bedömas för att avgöra den egna sårbarheten. Arbetet bör utgå från en tänkt händelse och därefter bedöma organisationens förmåga att:

- > förutse (exempelvis via omvärldsbevakning och underrättelse eller liknande),
- > upptäcka (personellt eller tekniskt skydd),
- > motstå (mekaniskt skydd),
- > hantera (kontinuitetsplanering, personella resurser, insatstider, dynamiska skydd, krishantering med mera) samt
- > återhämta (kontinuitetsplanering).

Se kapitel 7 för mer information om kontinuitetsplanering.

HOTBILDSANALYS

Hotbilden är en färskvara och kan förändras snabbt. Det krävs därför att man kontinuerligt bedömer hoten mot verksamheten och tar fram både reella och potentiella hotbilder.

Bedömning av en illasinnad aktör sker avseende:

- > avsikt,
- > förmåga och
- > möjlighet.

Till hjälp vid hotbilsbedömning bör både interna och externa resurser användas, exempelvis:

- > polis,
- > branschorganisationer,
- > säkerhetsnätverk,
- > egen och/eller extern omvärldsbevakning samt
- > information från tillbuds- och avvikelserapportering.

För mer information om riskanalyser och metoder rekommenderas exempelvis **Handbok för riskanalys** utgiven av Myndigheten för samhällsskydd och beredskap (MSB).

4. PERSONALSÄKERHET

FÖRUTSÄTTNINGAR FÖR EN SÄKER ORGANISATION

En förutsättning för en säker organisation är en välgrundad etik för hela företaget oavsett ledningsnivå eller enskild befattning.

Vanligtvis bygger säkerhetsarbetet på att företagen skyddar sig mot externa risker. Det är dock viktigt att inse att en del av ett företags skador orsakas av egen personal eller av personer som av annan anledning har tillträde till organisationen. Det är lätt att bortse från detta förhållande då det kan vara svårt att tänka sig att egen personal handlar illojalt. Vanliga orsaker till interna oegentligheter är brister i utbildning, lågt säkerhetsmedvetande, otydliga regler samt bristande uppföljning.

Enskilt viktigaste skyddet mot interna oegentligheter består i en företagskultur som uppmuntrar lojalitet, god moral och ömsesidig tillit hos chefer och medarbetare. Utan en säkerhetsmedveten personal kan det krävas att säkerhetsnivåerna ibland höjs så mycket att det blir både opraktiskt och olustigt att arbeta där, samtidigt som kärnverksamhetens genomförande försvåras. Detta innebär att man bör sträva efter en arbetsmiljö där kollegor och chefer bryr sig om sina medarbetare.

ANSTÄLLNING

Säkerhetsarbete påbörjas redan innan en anställning startar. Det är väl investerad tid och kostnad att informera sig om den tilltänkte och dennes bakgrund innan anställning startar. Även under anställningsintervjun bör frågor med bäring på säkerhet ställas. Exempelvis kring etik, förhållningssätt, vanor, intressen, relationer och ekonomiska förhållanden.

Referenser bör tas i den omfattning som är rimligt med tanke på vilket ansvar och vilka uppgifter som anställningen innebär.

TYSTNADSFÖRBINDELSE

Bestämmelser om sekretess är en väsentlig del av säkerhetsarbetet. Inga tveksamheter får råda om vad som är öppen, intern, företagshemlig eller kvalificerat företagshemlig information.

Som en del i detta är det lämpligt att de anställda, efter utbildning, får skriva under en tystnadsförbindelse. Tystnadsförbindelsen ska utformas beroende på vilken information den anställde har eller kommer att ha tillgång till. Innan undertecknandet av tystnadsförbindelsen bör en genomgång av förbindelsen göras med den anställde. Lämpligtvis görs detta i samband med den information om säkerhetsföreskrifter som bör ges i samband med nyanställning. Exempel på tystnadsförbindelse redovisas i bilaga.

SÄKERHETSPRÖVNING OCH REGISTERKONTROLL

För detaljer kring detta hänvisas till kapitel 8.

ANSTÄLLNINGENS UPPHÖRANDE

Det är lämpligt att genomföra ett avslutande samtal med personal i samband med att anställningen upphör. I detta samtal bör påpekas att den eventuella tystnadsförbindelse som skrevs under vid anställningens början fortsätter att gälla även efter anställningens upphörande.

I samband med att någon slutar ska det finnas rutiner för återlämnande av olika

typer av behörigheter och utrustning såsom dator, IT-behörigheter, nycklar, mobiltelefon, passerkort, tjänstelegitimation och så vidare.

PERSONAL FRÅN KONSULTBOLAG, ENTREPRENÖRER OCH INHYRDA

När affärsavtal tecknas med konsulter, underleverantörer och inhyrda är det viktigt att även ett avtal om sekretess och säkerhet tecknas. Sekretess- och säkerhetsavtal (motsvarande) tecknas med firmatecknaren för företaget/organisationen som avtal ska slutas med. För att ytterligare stärka betydelsen av hantering av sekretessbelagda uppgifter kan även ett personligt avtal med den enskilde tecknas. Exempel på sekretess- och säkerhetsavtal samt tystnadsförbindelse redovisas i bilaga.

INFORMATION OCH UTBILDNING

Information och utbildning är viktiga delar i det förebyggande säkerhetsarbetet. De anställda måste bli medvetna om de risker och hot som kan finnas på arbetsplatsen. Informationsarbetet bör dock bedrivas med eftertanke så att det inte motverkar sina egna syften. Målar man upp alltför stora hot och risker är det lätt att de anställda resignerar.

Utbildningarna bör anpassas till respektive målgrupp samt inriktas mot ett aktivt deltagande. Erfarenheter och synpunkter som inkommer från utbildningarna ska hanteras och det är viktigt med återkoppling till deltagarna.

HANTERING AV MISSBRUKSPROBLEM

Missbruk kan finnas i många former: droger, alkohol, spel med mera. Missbruket är farligt både för den som missbrukar men även för dennes omgivning. En vanlig missuppfattning är att missbrukare skulle vara socialt utslagna individer. Det finns exempel på väletablerade personer som i flera år lyckats dölja sitt missbruk för familj, vänner och arbetskamrater. Missbrukare kan utgöra säkerhetsrisker, dels genom att missbruket kan medföra att dessa personer begår misstag i sitt arbete, dels genom att de kan bli mottagliga för utpressning eller råka i ekonomiska svårigheter som de försöker lösa genom kriminella handlingar.

Enligt Arbetsmiljöverket ska arbetsgivaren tydliggöra vilka interna regler och rutiner som gäller om en arbetstagare uppträder påverkad av alkohol eller andra berusningsmedel (narkotika och vissa läkemedel). Arbetsgivaren ska även ha rutiner för missbruksrehabilitering. Arbetsgivarens ansvar framgår av 3 kap. 2§ arbetsmiljölagen (1977:1160).

För att underlätta hanteringen av missbruk måste det vara tydligt vilken policy som gäller, vad som ska göras vid misstanke eller upptäckt, vart man vänder sig, tystnadsplikt och så vidare. Det är även viktigt att alla anställda får utbildning i dessa frågor samt att särskilt chefer med personalansvar tränas i hantering av missbruksproblematik.

För ytterligare rådgivning och stöd hänvisas till EBRID (Energibranschens resurscentrum i alkohol- och drogfrågor).

VÅLD OCH HOT OM VÅLD

För att kunna skydda företagets personal från faror av skilda slag måste den som är säkerhetsansvarig känna till och förstå företagets verksamhet. Det är av stor betydelse att den som i sitt arbete riskerar att utsättas för hot, våld eller ökad risk får information om hur hotbilden ser ut i de aktuella fallen.

Varje företag bör ha rutiner som gör det möjligt att snabbt vidta åtgärder om våld och hot om våld inträffar. En polisanmälan görs normalt och följs av en utredning. De flesta säkerhetsföretag har särskilda personskyddsenheter och kan erbjuda hjälp och utföra hotbildsanalyser då personliga hot förekommer. Beroende på hotets art kan även säkerhetspolisen kontaktas.

Se även AFS 1993:2 **Våld och hot i arbetsmiljön**

RESERUTINER

Varje företag bör ha rutiner för tjänsteresor/utlandsresor. Förutom företagets egen research och bedömning av resesituationen bör man även nyttja svenska UD:s rese-rekommendationer.

Några grundläggande åtgärder är att:

- > inte i onödan skylta med företagets namn, resmål och ändamål för resan. Ta två omgångar kopior på pass och resehandlingar. Ta med den ena och lämna den andra på företaget.
 - > inför utlandsresan göra upp en telefon- och adresslista för resmålet som innehåller uppgifter om hotell, ambassad med mera och hur man ringer till Sverige.
 - > ta med uppgifter om nödvändiga mediciner och liknande.
 - > på företaget lämna in en resplan med tider, vem som ska besökas, vilket hotell som används och så vidare. Här måste också finnas uppgifter om närmast anhöriga (minst två stycken).
 - > ordna nödvändiga försäkringar och klarlägga innan utresa hur en eventuell sjukhusvistelse i utlandet ska regleras.
 - > inhämta information om landet som besöks. Följa de restriktioner/regler som förekommer kring exempelvis alkohol och litteratur. Undvika att gå ensam.
-

5. INFORMATIONSSÄKERHET

INFORMATION OCH INFORMATIONSSÄKERHET

Information är en tillgång som, liksom andra viktiga tillgångar i en organisation, har ett värde och följaktligen måste få ett adekvat skydd. Information förekommer i många former. Den kan exempelvis vara tryckt eller skriven, elektroniskt lagrad, skickad med post eller e-post, visad på film eller muntlig. Förutom information i administrativa system avses även styr- och reglersignaler för produktion och överföring av el, gas och värme, larm och larmöverföring, inställningar av reläskydd med mera.

Informationssäkerhet syftar till att skydda information mot förekommande hot, förhindra avbrott i verksamheten, minska skador och bidrar därigenom till att säkerställa organisationens verksamhet.

Oavsett vilken form informationen har eller det sätt på vilket den överförs eller lagras, måste den alltid ha ett godtagbart skydd.

Informationssäkerhet karaktäriseras som:

- > riktighet/tillförlitlighet – bevarande och skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga,
- > sekretess – säkerställande av att information är tillgänglig endast för dem som har behörighet för åtkomst,
- > tillgänglighet – säkerställande av att behöriga användare vid behov har tillgång till information och tillhörande tillgångar samt
- > spårbarhet – åtkomst och informationsöverföringar loggas eller på annat sätt märks (exempelvis genom signering) för att händelseförlopp ska kunna kontrolleras och kopplas till specifik person.



INFORMATIONSSÄKERHET

Informationssäkerhet syftar som tidigare nämnts till att skydda information mot förekommande hot, förhindra avbrott i verksamheten, minska skador och bidrar därigenom till att säkerställa organisationens verksamhet.

Information finns idag överallt. Exempel på information är tryckt material, tidningar, hemligstämplade dokument, signaler i driftsystem som styr processer i el- och värmeproduktion, styrning av apparater i ställverk eller styrning av säkerhetsinstallationer i kontorsmiljöer, muntlig information under diskussionen i fikarummet mellan kollegor eller under ett samtal i mobiltelefon på offentlig plats. Informationen flödar och därför är det viktigt att sätta upp handlingsplaner som gör att organisationen kan handskas på rätt sätt med denna.

IT-SÄKERHET

Ordet IT-säkerhet får ofta felaktigt samma betydelse som informationssäkerhet. Med IT-säkerhet menas de tekniska möjligheter som finns tillgängliga för att skydda företagets information som finns lagrat i IT-system. Det kan vara den brandvägg som skyddar organisationen från inkommande hot från Internet eller det viruskydd som används för att inte få in virus i organisationens datornätverk. IT-säkerhet är alltså de tekniska lösningar som skyddar hårdvara, mjukvara och datornätverk och som finns för att förhindra att obehöriga får åtkomst till organisationens information.

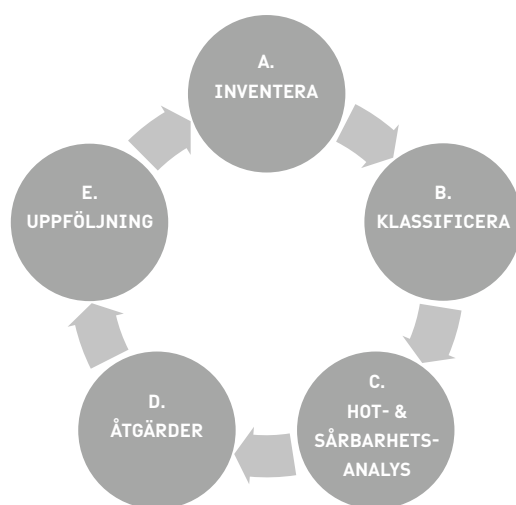
ADMINISTRATIV SÄKERHET

Den administrativa säkerheten omfattar regler och riktlinjer som företaget måste ställa på användarna.

Den omfattar hur tryckt material, tidningar, hemligstämplad information och samtal på offentliga platser ska behandlas/hanteras. Det kan också vara hur drift och underhåll ska ske på befintliga administrativa och processnära IT-system eller vilket ansvar som ställs på de roller som är definierade inom organisationen. Det är väldigt viktigt att personalen och användarna vet vilka regler och riktlinjer som finns och dessutom har en tydlig bild av och förståelse för varför dessa regler finns och varför de måste respekteras. Detta kan uppnås genom återkommande säkerhetsutbildningar och insatser för att höja medvetenheten.

SÄKRA FÖRETAGETS INFORMATIONSTILLGÅNGAR

För att säkra/skydda informationstillgångarna behöver ett antal olika steg gås igenom. De nedan förklarade stegen är inte på något sätt en fullständig beskrivning av allt som behöver göras utan snarare en utgångspunkt för idéer om hur det kan genomföras.



A. INVENTERA

En förutsättning för att kunna hantera risker är att man är medveten om vilka informationstillgångar som finns inom organisationen. Det är därför mycket viktigt att en komplett inventering av informationstillgångarna utförs. Ett hjälpmedel för att inventera är exempelvis systemet BITS Plus som kan hämtas ifrån MSB:s webbplats (www.msb.se).

B. KLASSIFICERA

Innan en hot- och sårbarhetsanalys genomförs måste verksamhetens krav på och beroende av ett informationssystem analyseras och dokumenteras (klassning). En klassningsmodell som kan användas för informationssystem är nedanstående. Den är enbart ett exempel och kan behöva justeras efter den egna organisationen. När en

klassning av informationssystemet har gjorts kan man börja med riskanalysen och genom denna bedöma vilka åtgärder som måste vidtas för att minimera/förhindra att skador uppstår.

Varje informationstyp ska klassas enligt tabellerna nedan oberoende av varandra.

Företagets strategiska planer hamnar på "Kvalificerat företagshemlig information" enligt sekretessklassningen men hamnar på basnivå i tabell 2.

Pressreleaser/tarifftryck hamnar på "Öppen information" i tabell 1, men hamnar på "Hög nivå" avseende riktighet och "Mellannivå" avseende spårbarhet i tabell 2.

TABELL 1. EXEMPEL PÅ SEKRETESSKLASSIFICERING

Säkerhetsaspekt/Kravnivå	Sekretess
Öppen information	Detta är information av sådan karaktär att dess spridning är önskvärd eller inte kan ha någon negativ inverkan på företaget eller för någon person. Informationen får spridas fritt.
Intern information	Information som kan medföra mindre allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig.
Företagshemlig information	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig.
Kvalificerat företagshemlig information	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig.

TABELL 2. EXEMPEL PÅ INFORMATIONSKLASSIFICERING

Säkerhetsaspekt/ Kravnivå	Riktighet/ tillförlitlighet	Tillgänglighet	Spårbarhet
Basnivå	Information som kan medföra mindre allvarliga konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som inte behöver vara åtkomlig inom X timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person.	Att unikt kunna spåra och logga på individnivå är mindre viktigt för att kunna följa upp vem eller vad som har gjort förändringar i systemet.
Mellannivå	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som inte behöver vara åtkomlig inom en halv dag, men inom högst X timmar för att inte medföra oacceptabla konsekvenser för egen eller annan organisation eller för enskild person.	Att unikt kunna spåra och logga på individnivå är viktigt för att kunna följa upp vem eller vad som har gjort förändringar i systemet.
Hög nivå	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som ska vara åtkomlig inom högst X minuter för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person.	Att unikt kunna spåra och logga på individnivå är kritiskt för att kunna följa upp vem eller vad som har gjort förändringar i systemet.

C. HOT- OCH SÅRBARHETSANALYS

Det första man ska göra är att bestämma vad som ska analyseras och syftet med analysen. Informationens skyddsbehov kan variera beroende på vilken typ av information som avses och aktuell hotbild, värdet av information och verksamhetens sårbarhet. Därför måste dokumenterade hot- och sårbarhetsanalyser genomföras regelbundet. Informationstillgången ska därefter hanteras och skyddas utifrån dess skyddsvärde så att risktagandet inte överstiger organisationens angivna normer.

Ett hot är när någon med avsikt negativt vill påverka verksamheten, medarbetarna eller dess roll i samhället. Om det finns en möjlighet för någon eller något att negativt påverka verksamheten är det en sårbarhet. Hot utgörs exempelvis av crackers som verkar genom Internet. Sårbarhet kan utgöras av informationstillgång (datasystem) kopplad till Internet. Om informationstillgången inte är kopplad till Internet finns alltså ingen sådan sårbarhet. Det krävs en sårbarhet för att hotet ska leda till en risk.

Risken ska värderas och beslut ska tas om hur risken kan hanteras.

D. ÅTGÄRDER

Det kan finnas flera vägar att välja mellan. Exempelvis kan man acceptera risken, åtgärda den eller kanske försäkra sig mot den. Följande åtgärder är exempel på hur man kan skydda sekretess, riktighet, tillgänglighet och spårbarhet:

Sekretess

Administrativa åtgärder:

- > Förvaring i säkerhetsskåp
- > Kurir/bud
- > Märkt med stämpel (olika nivåer)

Tekniska åtgärder:

- > Kryptering
- > Krypterad e-post
- > Behörighetsstyrd åtkomst

Riktighet

Administrativa åtgärder:

- > Attestregler
- > Rimlighetsbedömning
- > Utbildning personal

Tekniska åtgärder:

- > Checksummer/signering
- > Kontroll av inkommande information
- > Åtkomsträttigheter

Tillgänglighet

Administrativa åtgärder:

- > Inte nyckelpersonberoende
- > Planering inför exempelvis semester, viktigt att delegera
- > Kontinuitetsplan

Tekniska åtgärder:

- > Redundans
- > Avbrottsfri kraft
- > Avbrottsplan

Spårbarhet

Administrativa åtgärder:

- > Besökslistor och loggar
- > Tidsstämpling
- > Vaktbolag

Tekniska åtgärder:

- > Åtkomstloggar
- > Synkronisera klockor
- > Kameraövervakning

E. UPPFÖLJNING

För att kunna göra uppföljning måste det finnas riktlinjer, föreskrifter och instruktioner som är implementerade och som det går att mäta mot. Några exempel vad ett regelverk kan innehålla:

- > Incidenthantering
- > Informationssäkerhetspolicy
- > Riktlinjer administrativ säkerhet
- > Riktlinjer IT-säkerhet
- > Riktlinjer fysisk säkerhet

För att säkerställa att säkerhetskraven och skyddsåtgärderna som är implementerade är aktuella och tillräckliga måste de kontinuerligt utvärderas genom exempelvis sårbarhetsanalyser, omvärldsanalyser och riskanalyser. Regelverk uppdateras sedan baserat på resultatet från analyserna.

Det ska också regelbundet genomföras granskning av informationssäkerhet genom att analysera hur system förhåller sig till regler och riktlinjer. Vid incidenter bör det också utföras granskning för att utvärdera om gällande regelverk efterlevs.

Uppföljning är kanske den viktigaste delen av informationssäkerhetsarbetet eftersom det ger återkoppling inte bara till hur det fungerar i teorin utan även i praktiken.

UTBILDNING/MEDVETENHET

Utbildning och medvetenhet hos den egna personalen är en mycket viktig förutsättning. Utan detta kan personalen inte upprätthålla, underhålla och se till att informationen finns och är riktig.

Utbildning måste underhållas och uppdateras genom att personal utbildas i och för den information de behandlar. Det är inte minst viktigt att personalen håller sig medveten om aktuella hot och risker. Hoten mot informationstillgångarna ändras hela tiden och det är nästan helt omöjligt att ange vad det enskilt största hotet mot organisationen kan vara just för tillfället. Exempel på hot är insiders, virusattacker och externa organisationer som har specialiserat sig på intrång via Internet.

Som organisation kan man aldrig skydda sig fullständigt mot alla hot som finns och som tillkommer hela tiden. Det bästa man kan göra är att hålla sig uppdaterad om hotbilderna och möjligheterna att skydda sig och sedan göra det så svårt som möjligt för angriparna att lyckas. Ett sätt att minimera konsekvenser av oönskade händelser är att ha en dokumenterad, implementerad och utvärderad kontinuitetsplan för att kunna fortsätta verksamheten.

Se kapitel 7 för mer information om kontinuitetsplanering.

LÄS MER OM INFORMATIONSSÄKERHET

- > MSB:s rekommendationer **Basnivå för informationssäkerhet (BITS)**.
www.msb.se
- > Svensk standard. **Ledningssystem för informationssäkerhet – Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 17799:2005) och Krav (SS-ISO/IEC 27001:2006)**.
www.sis.se

BILAGOR

Bilagor som är relevanta för detta kapitel är i första hand:

- > Tystnadsförbindelse
- > Sekretess- och säkerhetsavtal
- > Checklista informationssäkerhet vid hantering av IT-system

6. ANLÄGGNINGSSÄKERHET

GRUNDKRAV

Anläggningar ska byggas så att de erbjuder ett väl avvägt skydd för personal, information, egendom, affärspartners och kunder. Skyddet ska utformas så att det försvårar för obehöriga att få tillträde till företagets skyddade delar, att göra inbrott, sabotera eller komma åt företagshemlig information.

Med anläggning avses de anläggningar som är avsedda för produktion, transmission och distribution av el, gas och värme (värme-, kraftvärme-, värmekraft- och vattenkraftverk samt transformator-, kopplings-, mät- och reglerstationer och driftcentraler). Med anläggningar avses också de lokaler som är viktiga för verksamheten exempelvis kontor, förråd och datacentraler. För kärnkraftsanläggningar gäller även särskilda bestämmelser utfärdade av Strålsäkerhetsmyndigheten.

En god anläggnings säkerhet uppnås genom att utförda riskanalyser resulterar i en väl genomtänkt åtgärdsplan. Teorin bakom detta beskrivs i kapitel 3.

När säkerhetsskyddsåtgärder vidtas krävs kunskap och eftertanke för att den totala säkerhetsskyddsnivån ska bli optimal både vad gäller ekonomi och säkerhet. En viktig faktor vid valet av säkerhetsskyddsnivå är anläggningens betydelse för företaget samt regional och nationell energiförsörjning. I detta kapitel rekommenderas vissa åtgärder och det är viktigt att notera att allt mekaniskt skydd är forcerbart. Viktiga anläggningar bör därför kompletteras med tekniskt skydd, eventuellt kombinerat med personell bevakning. Utformning av skydd påverkas i hög grad av hur utsatt anläggningen är för olika former av kriminella handlingar.

Skydd av energiförsörjningens anläggningar kan också dimensioneras efter krav i säkerhetsskyddslagen om tillträdesbegränsning.

BETYDELSEKLASSNING

För att uppnå en balanserad säkerhetsskyddsnivå krävs att respektive anläggningsägare eller verksamhetsansvarig genomför en betydelseklassning av sina anläggningar. Betydelseklassningen är beskriven i kapitel 8.

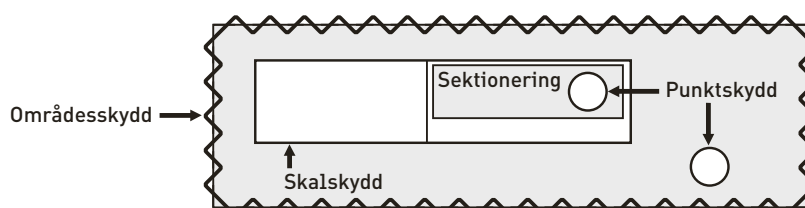
SKYDDSOBJEKT

Länsstyrelsen kan besluta att en anläggning ska vara skyddsobjekt efter att anläggningsägaren ansökt om detta, se vidare i kapitel 8.

GRUNDLÄGGANDE SKYDDSKRAV

Anläggningsanpassade skyddskrav måste ställas både på befintliga anläggningar, vid reinvesteringsarbeten och vid projektering av nya anläggningar. En anläggnings betydelse och utsatthet utgör då grunden för arbetet.

Skissen nedan beskriver de olika former av skydd som kan bli aktuella för en anläggning.



De grundläggande skyddsdefinitionerna för en anläggning är följande:

Områdesskydd

Utgörs av inhägnaden runt anläggningen som också ofta utgör anläggningens legala gräns.

Krav på fysiska barriärer måste vägas samman med åtgärder för teknisk bevakning och personella insatser. Långa insatstider vid larm medför högre krav på områdes- och skalskydd.

Oavsett vilken typ av områdes- och skalskydd som används kan detta forceras. Skyddet bör vara utformat så att det försvårar tillträdet (förlänger angreppstiden) och att det vid tillsyn eller uttryckning efter larm lätt kan konstateras om försök till intrång skett.

Skalskydd

Utgörs av anläggningens omslutningsytor, det vill säga ytterväggar med fönster, dörrar och tak med mera.

Sektionering

Uppdelning i sektioner (byggnadstekniskt och i larmsektioner) är ett definierat område där skyddsåtgärder vidtagits.

Punktskydd

Exempelvis dator- och telerum, master, nyckelpersonals arbetsrum, viktig verksamhet, säkerhetsskåp och så vidare. Skyddet kan bestå av exempelvis rörelselarm eller övervakningskamera.

FYSISKA SKYDDSÅTGÄRDER

I nedanstående avsnitt ges endast grundläggande information om de vanligaste fysiska skyddsåtgärderna. Med fysiskt skydd avses både mekaniskt skydd (A) och tekniskt skydd (B).

I Svenska Kraftnäts "Vägledning Fysiskt Grundskydd" ges råd och rekommendationer på åtgärder för att skydda anläggningar. Där finns även länkar till de normer, förordningar och lagar som berörs i denna vägledning.

A. MEKANISKT SKYDD

Med mekaniskt skydd avses exempelvis galler, grindar och utrustning som passivt ska försvåra att en obehörig person kommer åt, eller in i, en anläggning. Viktigt är att det mekaniska skyddet har samma skydds nivå över hela anläggningen.

Stängsel

Syftet med stängsel, som är en del av områdesskyddet, är att det avgränsar områden och styr person- och fordonsflöden till bestämda platser. Stängsel försvårar intrång till objekt och anläggningar och tjänar som skydd för oavsiktligt inträde. Det utgör även en legal avgränsning innanför vilken inga obehöriga får vistas utan tillstånd. Ett förbud meddelas genom att stängslet skyltas med förbudsskyltar.

Minimikraven för stängsel vid driftrum finns formulerade i starkströmsföreskrifterna, men enbart utifrån elsäkerhetsaspekten. Ett sådant stängsel erbjuder ett dåligt skydd mot skadegörelse, stöld och sabotage. Viktiga anläggningar bör därför ha ett mera svårforcerat stängsel. Ett helsvetsat stängsel – palissadstängsel – eller ett stängsel med någon form av tekniskt skydd bör övervägas.

Fasader och väggar

Vid konstruktion av väggar bör man ta hänsyn till skydds nivån för vitala anläggningsdelar och vilka övriga skyddsåtgärder som bör vidtas.

Fönster

Fönsterglas finns i olika säkerhetsklasser inom olika säkerhetsområden (vandalisering, inbrott, skottsäkra). Fönster bör installeras så att de inte kan monteras bort utifrån. Öppningsbara fönster bör ha godkänd låsanordning, avsedd för ändamålet.

I utrymmen av vital betydelse bör fönster i möjligaste mån undvikas, framför allt där husets yttervägg utgör en del av områdesskyddet.

Fönster kan kompletteras med galler eller annat inkrypningskydd eller med tekniskt skydd.

Dörrar och portar

En mycket vanlig angrepps- och reträttväg vid inbrott är portar och ytterdörrar. Dörrar indelas enligt standard i flera dörrklasser, beroende på skydds krav. Antalet dörrar för inpassering bör begränsas och om möjligt bör endast en dörr användas som entrédörr.

Entrédörr/port till en anläggning bör vara dimensionerad så att den inte går att forcera utan svårighet. Fönster i dörren ska undvikas. Detta gäller framförallt i dörrar som ligger mot undanskymda platser. En ytterdörr av trä kan förstärkas genom beklädnad med stålplåt på utsidan eller utrustas med gallergrind på insidan. Den bör också förses med brytskydd. Dörrar som öppnas utåt bör förses med bakkantssäkring. Dörren bör vara av samma klass som skalskyddet i övrigt.

Dörrar till drift/datacentraler och övriga vitala utrymmen bör hållas låsta. Dörrar försedda med passagekontroll – kortläsare – bör utrustas med dörrstängare.

Lås och nycklar/nyckelkort

Ytterdörrar och dörrar till vitala utrymmen ska vara försedda med godkända låsenheter. Vald skydds nivå för utrymmet styr antalet samt klassen på låsenheter per dörr/port.

Nycklar/nyckelkort bör endast tilldelas behörig personal och mot kvitto. Det är viktigt att föra register över utlämnade nycklar/nyckelkort. Varje nyckel/nyckelkort utgör en säkerhetsrisk och endast den som har behov av egen nyckel/nyckelkort bör därför tilldelas en.

Tilldelad nyckel/nyckelkort bör förvaras oåtkomligt för obehöriga och inte lånas ut eller kopieras. Förlust av nyckel/nyckelkort bör omgående anmälas. Reservnycklar/nyckelkort och kvittenser bör förvaras i säkerhetsskåp hos den som har utsetts till nyckelansvarig.

B. TEKNISKT SKYDD

Med tekniskt skydd avses exempelvis elektroniska larm, övervakningskameror och utrustning som ska larma eller varna om en person kommer in i en anläggning.

Larm och kameror

Tillträdesskydd kan kompletteras med inbrottslarm och eventuellt ett överfallslarm i någon form. Larmet kan överföras till en larmmottagare, så kallat centralanslutet larm. Överföringen vid viktiga anläggningar bör ske via övervakad ledning – alternativt kan två skilda överföringssystem övervägas. Larm kan kompletteras med kameraövervakning. Observera att vid montering av kamera gäller i tillämpliga delar bestämmelserna i lagen om allmän kameraövervakning om inte anläggningen är ett skyddsobjekt.

Stängsel kan, vid viktigare anläggningar, vara kombinerat med ett larmat elstängsel och/eller bildövervakning. En kombination av larm och kameraövervakning ger larmmottagaren möjlighet att se vad som utlöst larmet. För att undvika falsklarm bör larmområdet vara innanför stängslet.

Belysning

En viktig del för skyddet av en anläggning är belysning. En upplyst anläggning i kombination med larm och kameraövervakning gör intrång lättare att uppmärksamma. Belysningen kan antingen vara kontinuerlig eller startas av exempelvis rörelsedetektorer. Belysning är en viktig parameter för kamerainstallationer och måste därför anpassas för att nå önskad effekt. Om belysningen tänds vid larm är det ibland tillräckligt för att avskräcka och avbryta ett intrångsförsök.

Övriga larm

Utrymmen där det kan förvaras företagshemliga handlingar, viktig materiel eller dyrbara verktyg bör förses med larm.

Ett enkelt lokalt larm, siren eller belysning, kan vara alternativa tillträdes- och inbrottskydd. Enkla lokala larm kan vara lämpligt på verktygs- och materielcontainer vid tillfälliga arbetsplatser. Observera att hänsyn till närboende måste tas vid anordnande av lokalt larm.

För särskilt utsatt personal kan även inbrotts- och överfallslarm i bostaden övervägas.

Anlita endast auktoriserade larmföretag.

Larmcentraltjänster

Larm samt bilder från kameraövervakningen kan terminera antingen hos egen driftcentral eller hos ett auktoriserat bevakningsföretag. Man kan även välja lösningen att kombinera båda dessa alternativ där exempelvis larm på dagtid terminerar hos driftcentralen medan det under övrig tid terminerar hos bevakningsföretaget. I detta fall är det vanligt att bevakningsföretaget kontaktar företaget vid skarpa larm.

Driftcentralens fördel är att de har god lokalkännedom medan nackdelen är att de kan bli störda i sin driftledningsfunktion av diverse falsklarm vilket kan leda till att inkomna skarpa larm inte hanteras tillräckligt snabbt. Bevakningsföretagets fördel är att de har stor erfarenhet av att hantera larm och dess nackdel är att de kan sakna lokalkännedom om en anläggning.

PERSONELL TILLSYN OCH BEVAKNING

Personell tillsyn (rondering), bevakning och tekniska skyddsåtgärder bör komplettera varandra så att en balanserad säkerhet uppnås för en anläggning.

Tillsyn av en anläggning kan utföras av egen personal, entreprenörer eller av bevakningsföretag och innebär att man i samband med besök kontrollerar stängsel och utrymmen som ska vara låsta samt att inbrott/försök till inbrott eller skadegörelse inte har skett.

Bevakning av en anläggning kan ske enligt följande:

- > Stationär bevakning
- > Ronderande bevakning
- > Larmutryckning

Bevakning ska utföras av auktoriserat företag som är godkänt av länsstyrelsen. Bevakningsföretag utnyttjar utbildade väktare för bevakning av anläggning. Anläggningsägare bör ställa tydliga krav över hur bevakning ska utföras för att ge underlag för den instruktion bevakningsföretaget ska upprätta. Instruktionen ska godkännas av anläggningsägaren.

För bevakning av skyddsobjekt får endast skyddsvakt användas. Till skyddsvakt utses person som genomgått skyddsvaktutbildning och som godkänts av länsstyrelsen. Skyddsvakt utrustas efter godkännande av länsstyrelsen med batong och handfängsel och kan även i vissa fall, efter polisens godkännande genom utfärdad licens, utrustas med vapen och/eller hund. Företaget ska strikt följa Rikspolisstyrelsens föreskrifter och allmänna råd (FAP 579-3) om utbildning och utrustning av skyddsvakter samt för bevakning av civila skyddsobjekt. Utryckning till skyddsobjekt vid larm behöver inte ske med skyddsvakt.

LUCKOR, LUFT- OCH VATTENINTAG

Om luft- eller vattenintagen är så stora att någon kan krypa igenom dem bör man montera inkrypningskydd med stålgaller eller motsvarande. Dessa mekaniska åtgärder kan även kombineras med tekniskt skydd i form av larm och/eller kameraövervakning.

MASTER OCH KOMMUNIKATIONSANLÄGGNINGAR

En mast inklusive manöverbyggnad bör om möjligt placeras innanför anläggningens områdesskydd. Om detta inte är möjligt bör den förses med eget stängsel och, beroende på betydelse, i vissa fall larm. Master bör inte placeras så att de kan fällas över känsliga och vitala anläggningsdelar.

För att förhindra skadegörelse av vitala delar i en mast bör den förses med ett överklättringsskydd till en höjd av cirka 2,5 m över marknivån. Luckor till klätterskyddet bör förses med lås med en relevant låsklass.

Kablar bör skyddas upp till 3,5 m höjd över marken på motsvarande sätt eller genom plåtinklädnad.

KABLAGE

Kabelgravar utanför inhägnat område bör undvikas. Rörförläggning ger ett bättre skydd. Täckning till kabelgravar bör utföras i betong. Ett ökat skydd mot bland annat antändning kan erhållas genom att kabelgravarna fylls med sand. Kabelbrunnar bör förses med lås.

Kablar som inte är nergrävda bör skyddas med stålrör.

KRAFTLEDNINGAR

Över större avstånd är kraftledningar mycket svåra att skydda mot åverkan. För kortare sträckor kan kablifiering vara ett alternativ. I speciellt utsatta områden kan kameraövervakning användas. För reparation av stolpar och ledningar bör reservmaterial finnas i lager samt nödvändiga reparationsresurser finnas tillgängliga. En ökad uppmärksamhet samt rapportering kan i bästa fall motverka konsekvenser av åverkan.

BEFOGENHETER ATT INGRIPA

”Om den som begått brott varpå fängelse kan följa, påträffas på bar gärning eller flyende fot, får han gripas av envar. Envar får också gripa den som är efterlyst för brott. Den gripne skall skyndsamt överlämnas till närmaste polisman.”

(24 kap. 7 § rättegångsbalken)

Var och en har alltså rätt att gripa den som begått brott om gärningsman påträffas på bar gärning eller när han flyr från brottsplatsen under förutsättning att fängelse kan följa på brottet. Kravet på fängelsestraff innebär att det bara behöver ingå i straffskalan för det aktuella brottet. Både exempelvis snatteri och skadegörelse utgör av den anledningen gripandeskäl. Med ”bar gärning” menas att gärningsman just då utövar brottet och ”flyende fot” innebär att brottet är nyss begånget och att det inte får råda någon som helst tvekan om vem som begått brottet. Helst bör förföljare inte tappa ögonkontakt med brottslingen för att gripandet ska anses ha skett på flyende fot. Vid gripande får inte mer våld än nödvändigt tillgripas. Om en person misstänks för exempelvis stöld, men ingen sett vederbörande begå brottet, får inget ingripande ske utan polis ska tillkallas.

Envarsingripande

Den som ingriper:

- > ska ha sett brottet begås,
- > får inte riskera sitt och andras liv,
- > får använda försvarligt våld och
- > får inte verkställa straff, endast gripa.

Även en väktare har envars rätt att gripa, men han har dessutom uppdragsgivares befogenheter gentemot anställda när han utför ett uppdrag enligt fastställd instruktion.

Skyddsvakt har utöver envarsrätten betydligt större befogenheter att ingripa.

Skyddsvakts befogenheter med stöd av Skyddslag (2010:305) innebär möjlighet att:

- > kontrollera behörighet.
- > avvisa och avlägsna,
- > tillfälligt omhänderta,
- > kroppsvisitera,
- > beslagta samt
- > gripa.

Strängare straff utdöms normalt för den som misshandlar en väktare eller skyddsvakt.

Nödvärnsrätt

”Gärning som någon begår i nödvärn utgör brott endast om den med hänsyn till angreppets beskaffenhet, det angripnas betydelse och omständigheterna i övrigt är uppenbart oförsvarligt.” (24 kap. 1 § brottsbalken)

Rätt till nödvärn föreligger mot:

- > ett påbörjat eller överhängande angrepp på person eller egendom,
- > den som med våld eller hot om våld eller på annat sätt hindrar att egendom återtas på bar gärning,
- > den som olovligen trängt in i eller försöker tränga in i rum, hus, gård eller fartyg samt
- > den som vägrar lämna annans bostad efter tillsägelse.

Om någon handlar enligt nödvärnsrätten utdöms inte straff fast det annars är brottsligt att handla så. Observera att det våld som tillgrips ska vara försvarligt.

Enligt nödvärnsrätten får man alltså med våld föra ut en person som olovligen tränger in på en anläggning (arbetsplats). Observera att det inte får tillgripas mer våld än vad nöden kräver, dvs. en proportionalitetsavvägning. Ett förbud måste meddelas genom exempelvis skyltning, stängsel eller låsta dörrar. Vid bristfällig inspiseringskontroll och dålig skyltning är det annars svårt att hävda att någon kommit in olovligen.

7. KRISBEREDSKAP

Detta kapitel behandlar övergripande företagets krisberedskap. I denna text görs ingen skillnad på vilken typ av kris som företaget drabbas av utan kris ses här utifrån ett verksamhetsperspektiv.

Enligt förordningen (2006:942) om krisberedskap och höjd beredskap, definieras krisberedskap som förmågan att genom utbildning, övning och andra åtgärder samt genom den organisation och de strukturer som skapas före, under och efter en kris kunna förebygga, motstå och hantera krissituationer.

RISKIDENTIFIERING

Det finns alltid risker som kan orsaka en kris med långtgående konsekvenser för medarbetare, egendom, miljö, ekonomi eller varumärke. Kriser kan vara både internt och externt genererade, ofrivilliga genom olyckshändelser eller medvetet skapade. Händelser som kan leda till kriser kan ha sitt ursprung i olika bakomliggande orsaker såsom:

- > människa
- > teknik
- > natur

För att identifiera dessa risker behöver analyser genomföras i form av risk- och sårbarhetsanalyser. Resultatet av dessa ligger sedan till grund för handlingsplaner. För vägledning se även kapitel 3.

Trots alla vidtagna förebyggande åtgärder (i form av bland annat risk- och sårbarhetsanalyser och från dessa framtagna rutiner och handlingsplaner) finns det alltid en kvarvarande risk att någonting allvarligt inträffar som förbisetts. För att ha förmåga att hantera även en sådan situation måste det i förväg vara bestämt vem eller vilka som ska agera och var i organisationen en sådan situation ska hanteras. Krishanteringens fokus ligger i att lindra konsekvenserna av det inträffade.

Krisledning och -hantering kan se olika ut beroende på företagets storlek. I det mindre företaget är det kanske delar av företagets ledningsgrupp som även utför den operativa krisledningen. I ett större företag är det strategiska och operativa omhändertagandet sannolikt delat på olika grupper.

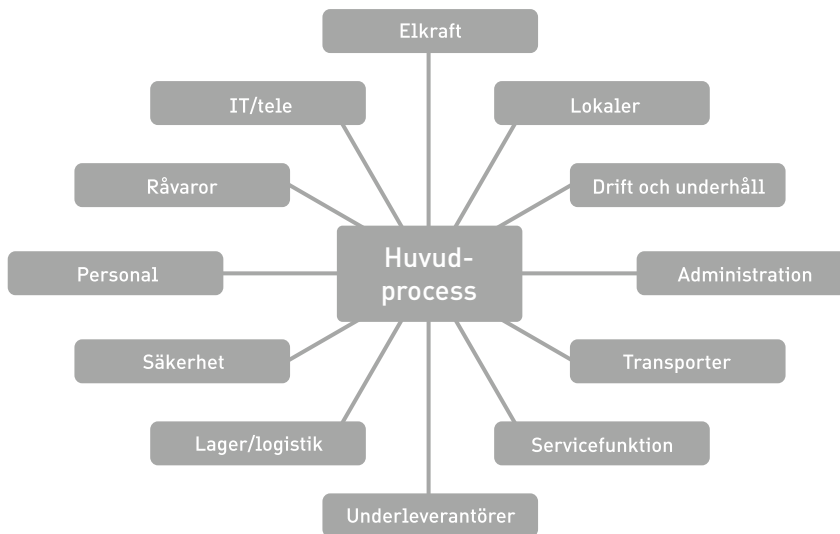
KONTINUITETSPLANERING

I traditionellt säkerhetsarbete ingår normalt förebyggande och skadebegränsande åtgärder. Ytterligare en dimension behöver läggas till och det är förmågan att överleva en inträffad skada genom att snabbt kunna komma tillbaka med delar av eller hela verksamheten.

En metod för att säkerställa företagets leveransförmåga vid skada eller avbrott är kontinuitetsplanering. Det innebär att företaget trots ett avbrott ska kunna leverera de tjänster och produkter som är viktigast för företaget, dess kunder och samhället. Det vill säga att ha en Plan B och kanske även en Plan C.

Genom att analysera huvudprocess och alla stödprocesser i en verksamhet kan företaget klargöra vilka förutsättningar som måste finnas för att kunna bedriva denna typ av verksamhet. När dessa förutsättningar har identifierats, finns ett behov av att säkerställa att förutsättningarna även fungerar vid ett avbrott. Detta kan åstadkommas via olika skyddsåtgärder eller genom att skapa redundans.

FIGUR 1: Ett exempel på olika stödprocesser i en verksamhet. I varje stödprocess/funktion klargörs skyddsnivån och grad av redundans.



KRISDEFINITION FÖR ETT FÖRETAG

Exempel på definition av kris för ett företag:

”En oförutsedd händelse eller en händelse som inte kan hanteras inom ordinarie organisation och med ordinarie resurser, utan som riskerar att orsaka stor skada på människa, miljö, ekonomi eller på varumärket.”

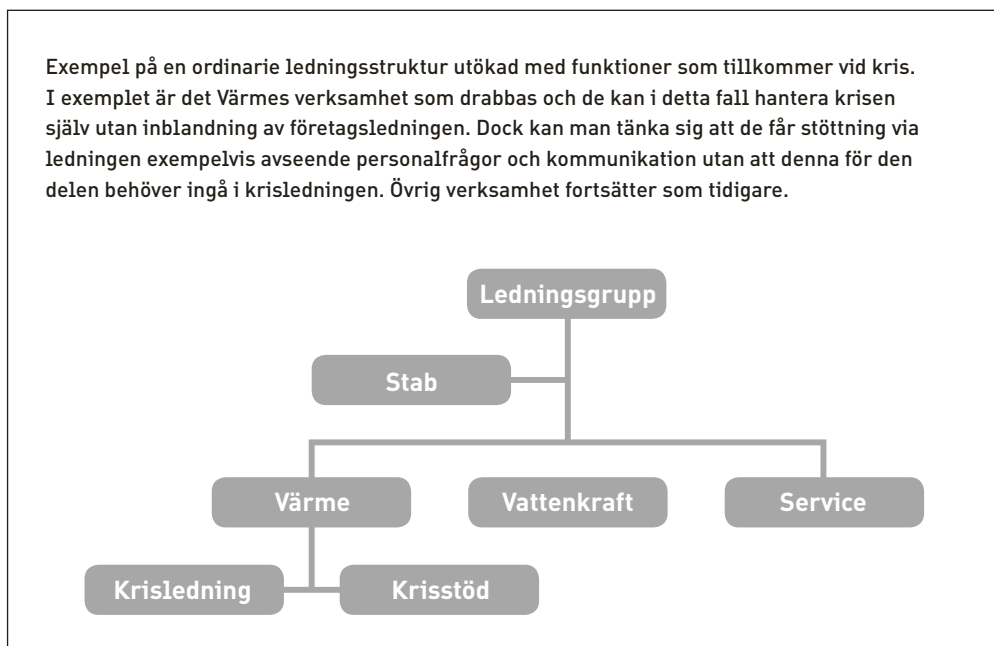
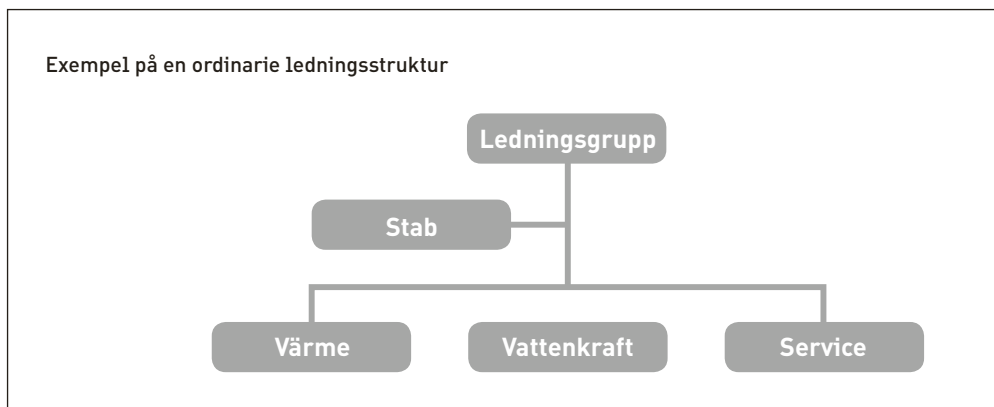
KRISHANTERING

Erfarenheten säger att företagets framgång i kris alltid avgörs av hur förberedd organisationen är, vilka resurser den har till förfogande och ledarskapet i krisen. Förmågan att hämta in information, värdera situationen, fatta riktiga beslut utan dröjsmål och förmågan att kommunicera med omgivningen vilar helt på ledningens kunskaper och beredskap. Företagets krishanteringsförmåga bygger således på både strategisk och operativ förmåga.

KRISLEDNINGSFÖRMÅGA

Med krisledningsförmåga avses förmågan att inom ett verksamhets- eller ansvarsområde, vid allvarliga störningar, leda den egna verksamheten. I detta ingår att fatta beslut, sprida snabb och tillförlitlig information samt vid behov kunna medverka i samordning och koordinering med andra aktörer.

Nedan redovisas exempel på ledningsstruktur för ordinarie verksamhet samt för krisledning.



KRISSTÖD

Med krisstöd avses det psykiska och sociala omhändertagande som behöver vidtas i samband med olyckor, akuta krissituationer och liknande allvarliga händelser som kan utlösa krisreaktioner. Se bland annat arbetsmiljöförordningen (1977:1166) samt Arbetskyddsstyrelsens föreskrift (AFS 1999:7) **Första hjälpen och krisstöd**.

UTBILDNING OCH ÖVNING

För att säkerställa att organisationen är förberedd så långt det är rimligt och möjligt krävs att den är utbildad och övad. Utbildning och övning är även ett viktigt instrument för att säkerställa att de planer och checklistor som finns är operativt användbara samt att krisledningsrum (eller motsvarande) fungerar tillfredsställande. Det finns ett stort urval av övningsmetodiker man kan använda men det viktigaste är att dessa är anpassade efter företagets förmåga och förutsättningar.

8. SAMHÄLLSVIKTIG VERKSAMHET

Samhället är idag uppbyggt av en rad sammansatta verksamheter vars funktionalitet är helt avgörande för hur väl samhället i sin helhet fungerar. Dessa verksamheter tillhandahåller så viktiga tjänster och produkter att om de drabbas av störningar eller avbrott kan människors hälsa och liv och möjligheten att värna samhällets grundläggande värden riskeras.

Samhällsviktig verksamhet ur ett krisberedskapsperspektiv är verksamhet som uppfyller det ena eller båda av följande villkor:

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

De samhällsviktiga verksamheterna består i stor utsträckning av olika flöden och processer som på olika sätt utnyttjar infrastrukturer, exempelvis el- och telekablar och vägar. Avbrott i en verksamhet påverkar dessutom andra samhällsviktiga verksamheter. Exempel på samhällsviktiga verksamheter är energiförsörjningen, vattenförsörjningen och transportsystemen.

En väl fungerande energiförsörjning är av grundläggande betydelse för stora delar av samhällets verksamhet och en förutsättning för Sveriges ekonomiska och sociala utveckling. El är en förutsättning för nästan all annan energiförsörjning och ofta en förutsättning för att andra tekniska system ska fungera. Långvariga och omfattande elavbrott kan allvarligt drabba exempelvis telekommunikationer, transporter, industriproduktion, sjukvård, betalnings- och IT-system och uppvärmning. Störningar i funktionerna kan orsaka betydande materiella skador och ekonomiska förluster. Under svåra väderleksförhållanden kan elavbrott också vara en fara för individers hälsa och överlevnad.

Med tanke på energiförsörjningens betydelse för andra viktiga samhällsfunktioner får därför långvariga avbrott i energiförsörjningen anses inta en central del i samhällets säkerhets- och beredskapsplanering.

Stora delar av elförsörjningen och andra delar av energiförsörjningen är därmed att räkna som samhällsviktig verksamhet. För samhällets säkerhet är det avgörande att aktörer som bedriver samhällsviktig verksamhet har en kunskap om vilka hot och risker som finns i deras respektive verksamhet samt vilka metoder som kan användas för att hantera dessa. Med utgångspunkt i de analyser som kontinuerligt måste ske bör de verksamhetsansvariga fastställa och redovisa vilken verksamhetsnivå som kan anses rimlig även om störningar inträffar. Därefter bör den verksamhetsansvarige vidta åtgärder så att denna nivå kan upprätthållas.

SKYDD AV KRITISK INFRASTRUKTUR

Begreppet skydd av kritisk infrastruktur, som används framförallt inom EU och i andra internationella sammanhang, kan till viss del kopplas till det arbete som bedrivs

avseende samhällsviktig verksamhet inom EU och för det svenska krisberedskapssystemet. För att kunna upprätthålla en grundläggande funktionalitet i samhället måste ytterst de verksamheter som är viktiga för samhället kunna fungera och inte enbart den infrastruktur som helt eller delvis bär upp verksamheten. Skydd av kritisk infrastruktur syftar till att minska sårbarheter genom ett förebyggande arbete, vilket skapar en bättre säkerhet i samhället. Frågan om skydd av samhällsviktig verksamhet handlar lika mycket om infrastrukturens robusthet som om att efter ett avbrott eller en störning ha förmåga att återställa funktionaliteten.

SKYDDSOBJEKT

Samhällsviktig infrastruktur kan enligt Skyddslag (2010:305) av länsstyrelse beslutas vara skyddsobjekt. Beslut om skyddsobjekt tas av länsstyrelsen i det län där anläggningen ligger efter initiativ från ägaren och nyttjaren i de fall anläggningen upplåtits till särskilt nyttjande. Ägs anläggningen av annan än staten krävs ägarens medgivande för att anläggningen ska kunna förklaras vara skyddsobjekt. Skyddet inriktas mot sabotage, terrorism och spioneri.

Fördelar för verksamhet vid en anläggning som beslutats vara skyddsobjekt är:

- > utökade befogenheter vid säkerhetskontroller, bland annat kan det ställas hårdare krav på säkerhetsprövning av personal som arbetar vid anläggningen, inpasseringskontrollen och tillträdesskyddet kan också göras mer omfattande,
- > att verksamheten vid ett skyddsobjekt kan kräva prioritering från myndigheter exempelvis polis och kustbevakning vid behov av bevakning vid extra ordinära händelser som demonstrationer, hot, sabotage med mera. Vid för samhället extrema situationer kan även resurser från försvarsmakten begäras för bevakning,
- > uttryckning till skyddsobjekt kan prioriteras av polismyndighet,
- > att vid bevakning av ett skyddsobjekt ska skyddsvakt användas som i många situationer i och omkring skyddsobjektet har befogenheter motsvarande polisman. Vid rondering och tillsyn kan vanlig väktare eller egen personal användas. Kameraövervakning av ett skyddsobjekt får utföras utan särskilt tillstånd av länsstyrelsen,
- > att den som gör intrång på ett skyddsobjekt kan dömas till ett högre straff och
- > att verksamheten vid ett skyddsobjekt har lättare att beviljas beredskapsmedel för säkerhetshöjande åtgärder (förkortas BSÅ).

För verksamhet vid en anläggning som beslutats vara skyddsobjekt innebär detta även större ansvar och skyldigheter, bland annat i form av:

- > utökad administration, ansökan och kommunikation med länsstyrelser. Skyddsobjektsområdet ska också skyltas. Skyltning kan i sig också medföra ett ökat oönskat intresse för anläggningens betydelse och
- > utökad sekretess. Företagets uppgifter om anläggningen och uttagna skyddsobjekt bör klassas som lägst företagshemlig handling. För myndigheter och de företag som lyder under offentlighetsprincipen ska offentlighets- och sekretesslagen tillämpas.

Skyddsåtgärder vid ett skyddsobjekt och/eller samhällsviktig anläggning syftar alltså till att minska riskerna för sabotage, terroristbrott och spioneri. Ett skyddsobjekt är en samhällsviktig anläggning som har ett skyddsvärde med hänsyn till rikets säkerhet.

BETYDELSEKLASSNING

Betydelseklassningen är framtagen av elförsörjningen för klassning av elanläggningar. Denna betydelseklassning innehåller fyra klasser, från B1 till B4 där B4 innebär högsta säkerhetsklass. Nedan beskrivs detta med ett antal exempel på anläggnings typer inom respektive klass. Dessa exempel ska ses som vägledande men anläggningsägaren avgör själv efter genomförd säkerhetsanalys i vilken klass anläggningen ska placeras. Principerna för denna betydelseklassning kan även vara användbar för andra energianläggningar i tillämpliga delar.

TABELL 1: Elförsörjningens betydelseklassning för samhällsviktiga anläggningar.

Klass	Betydelse	Exempel
B1	Endast lokal betydelse	Nätstationer, förråd/depåer, lokalkontor.
B2	Regional eller stor lokal betydelse	Mindre KV, KVV, VV* . Större mottagningsstationer, kontor, förråd, radiolänkar. Fördelningsstationer (mellan 30-220 kV).
B3	Nationell eller stor regional betydelse	KKV, större KV, KVV, VV*. Större driftcentraler, kontrollrum, knutpunkter i regionnät, stamstationer, fördelningsstationer (från 220 kV), dammanläggningar, bränsledepåer (lagervolym > 150 000 m ³) och huvudkontor. För fjärrvärme viktiga pumpstationer och distributionsnät.
B4	Avgörande nationell betydelse	Viktiga knutpunkter i stamnätet, viktiga anläggningar för dödnätsstart.

*KKV=Kärnkraftverk, KV=Kraftverk, KVV=Kraftvärmeverk, VV=Värmeverk

SÄKERHETSSKYDD

Med säkerhetsskydd avses skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet. Säkerhetsskyddet utformas med stöd av säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633).

Säkerhetsskyddet omfattar det skydd som ska upprätthållas mot brott som kan hota rikets säkerhet.

”Rikets säkerhet” är ett begrepp som saknar en gemensam definition. Denna handbok tar fasta på definitioner från lagstiftning och säkerhetspolisen enligt följande:

Brott mot rikets säkerhet innebär brott mot vårt lands demokratiska system, nationella säkerhet och våra grundlagar.

Säkerhetsskyddet ska förebygga:

1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs – informationssäkerhet,
2. att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i punkt 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs – tillträdesbegränsning samt
3. att personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet – säkerhetsprovning.

Säkerhetsskyddet ska även förebygga terrorism, det vill säga våld, hot eller tvång för politiska syften, även om brottet inte hotar rikets säkerhet.

Bestämmelser om säkerhetsskydd finns i säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) samt i föreskrifter och allmänna råd som meddelas av Rikspolisstyrelsen. Rikspolisstyrelsen har utarbetat vägledningar för säkerhetsskydd och säkerhetsskyddad upphandling. I dessa beskrivs närmare begrepp och definitioner för säkerhetsskyddsarbetet, se www.sakerhetspolisen.se/publicerat.

SÄKERHETSPRÖVNING

Personal som deltar i verksamhet som har betydelse för rikets säkerhet ska säkerhetsprövas. Liksom säkerhetsskyddet regleras säkerhetsprövningen enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen. Säkerhetsprövning ska genomföras innan en person anställs eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet. Prövningen får även göras under pågående anställning.

Säkerhetsanalys av verksamheten visar vilken typ av anställning som ska placeras i någon av säkerhetsklasserna 1, 2 eller 3.

Klassindelningen sker utifrån vilken omfattning den anställde hanterar uppgifter som är av betydelse för rikets säkerhet:

1. i stor omfattning får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet
2. i omfattning som inte är obetydlig får del av uppgifter enl. 1
3. i övrigt får del av uppgifter som omfattas av sekretess och som är av betydelse för rikets säkerhet, om ett röjande kan antas medföra men för rikets säkerhet som inte endast är ringa

Generellt gäller att säkerhetsprövning av personal ska genomföras för alla verksamheter som har betydelse för rikets säkerhet. Detta gäller både nystartade och pågående verksamheter, alltså även om verksamheten från början inte varit säkerhetsklassad utan detta sker efter en tid och att personal redan finns anställd.

Med säkerhetsprövning avses uppgifter som framkommer vid:

- personbedömning – personbedömning ska grundas på den personliga kännedom som finns om den prövade.
- referenser – uppgifter som framgår av betyg, intyg och inhämtad information från exempelvis tidigare anställningar.
- registerkontroll – uppgifter som framkommit vid registerkontroll och eventuell särskild personutredning. Detta tillämpas vid kontroll mot säkerhetsklasserna 1 och 2. Registerkontroll får också göras utifrån skyddet mot terrorism. Registerkontroll får inte göras utan samtycke från den som säkerhetsprövningen gäller.

För säkerhetsprövning utifrån skyddet mot terrorism görs detta enligt säkerhetsskyddslagen 11 och 14 §§ samt SvKFS 2005:1. Detta gäller såväl anställd som anlitad personal.

SÄKERHETSSKYDDSCHEF

De organisationer som vid sin säkerhetsanalys har klarlagt att man har verksamhet av betydelse för rikets säkerhet ska utse en säkerhetsskyddschef som ska utföra kontroll över säkerhetsskyddet. Vid myndighet ska denna anställning vara direkt underställd myndighetens chef och för övriga verksamheter görs en stark rekommendation om samma placering (underställd VD).

Anställningarna som säkerhetschef och säkerhetsskyddschef behöver inte innehas av samma person men denna lösning är ofta förekommande och utgör inget formellt hinder.

BEREDSKAPSÅTGÄRDER I ELSYSTEMET (BSÅ)

Elberedskapslagen (1997:288) innehåller bestämmelser om beredskap vid produktion och överföring av el samt vid handel med el. Kompletterande bestämmelser ges i förordning (1997:294) om elberedskap och i föreskrifter utfärdade av Svenska Kraftnät.

Svenska Kraftnät är elberedskapsmyndighet och kan med stöd av elberedskapslagen besluta om beredskapsåtgärder i samband med förändringar i anläggningar och verksamhet. Vid sådana beslut sker finansiering, helt eller delvis, med elberedskapsmedel.

Några exempel på sådana åtgärder är:

- > förbättring av sabotageskydd,
- > förstärkning av stängsel,
- > reglerutrustning för ö-drift,
- > utökning av redundans i nät- och produktionsdrift,
- > lagring av bränslen för elproduktion,
- > installation av lokal kraft,
- > utbildningar och
- > krisövningar

Svenska Kraftnät har i föreskrift (SvKFS 1997:1) reglerat vilka åtgärder som ska anmälas och på vilket sätt anmälan ska göras. I föreskrift (SvKFS 1997:2) anges vad som kan utgöra beredskapsåtgärder och modell för finansiering.

Föreskrifter, publikationer och blanketter kan beställas från Svenska Kraftnät och laddas ner från dess hemsida (www.svk.se).

BILAGOR

- BILAGA 1** - LAGAR OCH FÖRORDNINGAR
- BILAGA 2** - BEFATTNINGSBESKRIVNING FÖR
FÖRETAGETS SÄKERHETSFUNKTION
- BILAGA 3** - EXEMPEL PÅ SKYDDSVÅRDA UPPGIFTER
- BILAGA 4** - TYSTNADSFÖRBINDELSE
- BILAGA 5** - SEKRETESS- OCH SÄKERHETSAVTAL
- BILAGA 6** - PERSONALHANTERING ANSTÄLLDA
- BILAGA 7** - PERSONALHANTERING ÖVRIG PERSONAL
- BILAGA 8** - ÅTGÄRDER VID BOMBHOT
- BILAGA 9** - CHECKLISTA INFORMATIONSSÄKERHET
VID HANTERING AV IT-SYSTEM
- BILAGA 10** - AVMILJÖ- OCH HÄNDELSEHANTERING

Bilaga 1

LAGAR OCH FÖRORDNINGAR

I detta avsnitt redovisas de viktigaste legala kraven som är av betydelse vid arbetet med säkerhet och säkerhetsskydd.

Observera att lagar och förordningar ändras. Kontrollera därför alltid tillämplig författnings aktuella lydelse. Fullständiga lagtexter går att hämta från exempelvis Notisum (www.notisum.se).

AKTIEBOLAGSLAGEN (2005:551)

Företagets VD har ansvaret för den löpande förvaltningen enligt styrelsens riktlinjer och anvisningar. Detta ansvar kan inte delegeras men det straffrättsliga ansvaret har bedömts möjligt att delegera under förutsättning:

§ att den till vilken ansvar delegerats har en självständig ställning (beslutsmässigt)

§ att den till vilken ansvar delegerats har en acceptabel kompetens och en adekvat utbildning samt att

§ ansvarsförhållandet tydligt framgår.

Detta innebär att all delegering bör ske i skriftlig form. I varje aktiebolag skall finnas arbetsordning för VD, styrelse, utskott och ordförande.

En revisor har i uppdrag att inför styrelsen revidera bolagets förvaltning (förvaltningsrevision).

ARBETSMILJÖLAGEN (1977:1160)

Lagen är en ramlag som innehåller grundläggande regler för arbetsmiljöns utformning. Lagen har fortlöpande ändrats genom åren. Grundtanken är att säkerställa en säker arbetsmiljö och främja arbetsmiljöarbetet i samverkan mellan arbetsgivare och arbetstagare.

ARBETSMILJÖFÖRORDNINGEN (1977:1166)

Innehåller kompletterande regler till arbetsmiljölagen. Arbetsmiljöverket meddelar föreskrifter som mer i detalj anger krav och skyldigheter beträffande arbetsmiljön.

BOKFÖRINGSLAGEN (1999:1078)

Lagen reglerar företagets skyldigheter vad gäller ekonomisk dokumentation (bl. a. skydd mot förändring och förlust).

ELBEREDSKAPSLAGEN (1997:288)

Lagen innehåller bestämmelser om beredskap vid produktion och överföring av el samt vid handel med el. Bestämmelserna reglerar ansvaret för den planering och de övriga åtgärder som behövs för att tillgodose elförsörjningen i landet vid höjd beredskap enligt lagen (1992:1403) om totalförsvaret och höjd beredskap.

Kompletterande bestämmelser ges i **förordning (1997:294) om elberedskap** och i föreskrifter utfärdade av Svenska Kraftnät.

FÖRORDNING (1997:294) OM ELBEREDSKAP

I förordningen ges kompletterande bestämmelser till elberedskapslagen. Av förordningen framgår att Svenska Kraftnät skall vara elberedskapsmyndighet och i denna egenskap får meddela de ytterligare föreskrifter som behövs för verkställigheten av elberedskapslagen och elberedskapsförordningen.

I förordningen anges bl. a. att beredskapsåtgärder kan avse

1. åtgärder för att säkra verksamhet, driftledning och verksamhetssamordning,
2. åtgärder för att möjliggöra reparationsarbeten,
3. åtgärder för att möjliggöra drift av separata delsystem,
4. åtgärder för att kunna genomföra förbrukningsregleringar,
5. åtgärder för att säkerställa tillförseln av el till prioriterade användare, och
6. fysiska skyddsåtgärder.

Elberedskapsmyndigheten, dvs. Svenska Kraftnät, får meddela närmare föreskrifter om åtgärder som kan utgöra beredskapsåtgärder.

ELLAGEN (1997:857)

Ellagen, som trädde i kraft den 1 januari 1998, innehåller bl. a. bestämmelser om elektriska anläggningar såsom koncessioner, systemansvar, balansansvar, elkvalitet, vissa regler om handel med el samt om elsäkerhet.

KOMMUNALLAGEN (1991:900)

Enligt denna lag skall offentlighets- och sekretesslagstiftningen tillämpas i aktiebolag och stiftelser där kommun eller landsting själva bestämmer. I aktiebolag och stiftelser där kommun eller landsting bestämmer tillsammans med någon annan, skall offentlighets- och sekretesslagstiftningen tillämpas bara i den omfattning som är rimlig med hänsyn till andelsförhållandena, verksamhetens art och omständigheterna i övrigt.

LAG (1998:150) OM ALLMÄN KAMERAÖVERVAKNING

I denna lag finns bestämmelser om användning av övervakningsutrustning såsom övervakningskameror och annan optisk övervakningsmateriel. Bl. a. ges bestämmelser till skydd för den personliga integriteten.

LAG (2006:544) OM KOMMUNERS OCH LANDSTINGS ÅTGÄRDER INFÖR OCH VID EXTRAORDINÄRA HÄNDELSER I FREDSTID OCH HÖJD BEREDSKAP

I denna lag ges bestämmelser om kommunernas och landstingens ansvar.

LAG (1984:3) OM KÄRNTEKNISK VERKSAMHET

Lagen innehåller bestämmelser om kärnteknisk verksamhet. Bl. a. sägs att säkerheten vid kärnteknisk verksamhet skall upprätthållas genom att de åtgärder vidtas som krävs för att förebygga fel i utrustning, felaktig funktion hos utrustning, felaktigt handlande, sabotage eller annat som kan leda till en radiologisk olycka, och förhindra olovlig befattning med kärnämne eller kärnavfall.

LAG (1990:409) OM SKYDD FÖR FÖRETAGSHEMLIGHETER

Med företagshemligheter avses information om affärs- eller driftförhållanden i en näringsidkares rörelse som personen håller hemliga och som, ifall de röjs, kommer att medföra skada för denne i konkurrenshänseende.

Lagen gäller i såväl myndigheternas näringsverksamhet som i offentligägda bolag och det privata näringslivet.

Den som bryter mot lagen kan dömas till böter eller fängelse för företagsspioneri och ådömas skadestånd. En förutsättning för fällande dom är att näringsidkaren har klassificerat informationen som hemlig och att gärningsmannen känt till detta.

Den som avslöjar ett brott som kan ge fängelsestraff eller som avslöjar ett allvarligt missförhållande kan inte straffas. Det vill säga att brottslig verksamhet inte kan döljas bakom den sekretess som företagshemligheten ger.

LAG (1993:1742) OM SKYDD FÖR LANDSKAPSINFORMATION

Innehåller bestämmelser om krav på tillstånd för flygfotografering och upprättande av databaser med landskapsinformation. Innehåller även bestämmelse om krav på tillstånd för spridning av flygbilder och andra sammanställningar av landskapsinformation. Med landskapsinformation menas lägesbestämd information om förhållanden på och under markytan.

FÖRORDNING (1993:1745) OM SKYDD FÖR LANDSKAPSINFORMATION

Innehåller närmare regler om bl. a. flygfototillstånd som prövas av Försvarsmakten samt regler om inrättandet av databaser med landskapsinformation där tillståndsfrågan prövas av lantmäteriverket.

LAG (2003:778) OM SKYDD MOT OLYCKOR

Bestämmelserna i denna lag syftar till att i hela landet bereda människors liv och hälsa samt egendom och miljö ett med hänsyn till de lokala förhållandena tillfredsställande och likvärdigt skydd mot olyckor.

LAGSTIFTNING TILL SKYDD FÖR IMMATERIELLA RÄTTIGHETER

Dessa författningar behandlar regler kring bl. a. upphovsrätt, patent, mönsterrätt, firmarätt och varumärkesrätt.

Det är viktigt att företaget reglerar vem som t. ex. äger ett datorprogram (anställda eller företaget). Om företaget använder utomståendes produkter felaktigt (t. ex. datorprogram) kan stora skadestånd utdömas.

NATURGASLAG (2005:403)

Denna lag innehåller bestämmelser om naturgasledningar, lagringsanläggningar och förgasningsanläggningar samt om handel med naturgas i vissa fall och om trygg naturgasförsörjning.

OFFENTLIGHETS- OCH SEKRETESSLAGEN (2009:400)

Denna lag gäller i det allmännas verksamhet, dvs. hos statliga och kommunala myndigheter. Vid tillämpningen skall även kommunala beslutande församlingar – liksom kommunala bolag och föreningar – jämföras med myndigheter.

De uppgifter om planläggning och beredskapsförberedelser som företag inom energiförsörjningen lämnar till en myndighet, enligt den skyldighet som beskrivs i lag om skyldighet för näringsidkare, arbetsmarknadsorganisationer m. fl. att delta i totalförsvarsplaneringen ovan, omfattas i regel av de offentlighets- och sekretessregler som gäller hos myndigheten. Om företaget vill att inlämnade uppgifter skall sekretessbeläggas hos myndigheten bör man uppmärksamma myndigheten om detta i samband med att uppgifterna överlämnas.

PERSONUPPGIFTLAGEN (1998:204)

Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen innehåller bl. a. bestämmelser om säkerheten vid behandling av personuppgifter.

SKYDDSLAG (2010:305)

Skyddslagen trädde i kraft den 1 juli 2010 då lagen (1990:217) om skydd för samhällsviktiga anläggningar m. m. upphörde att gälla.

Lagen innehåller bestämmelser om vissa åtgärder till skydd mot bl. a. spioneri, sabotage och terrorism. Den reglerar också vad som kan utses till skyddsobjekt (t. ex. energianläggningar), bestämmelser för tillträde och fotografering samt bevakning av skyddsobjekt.

Enligt övergångsbestämmelserna till skyddslagen skall byggnader och andra anläggningar som förklarats som skyddsobjekt före den 1 juli 2010 även fortsättningsvis anses vara skyddsobjekt, dock längst till utgången av 2014. För dessa skyddsobjekt gäller fortfarande den gamla lagen om skydd för samhällsviktiga anläggningar m. m.

LAG (1982:1004) OM SKYLDIGHET FÖR NÄRINGSIDKARE, ARBETSMARKNADS- ORGANISATIONER M. FL. ATT DELTA I TOTALFÖRSVARSPLANERINGEN

Lagen utgör den formella grunden för beredskapsförberedelser som görs inom företagen.

Den ålägger bl. a. kommuner och ägare eller innehavare av industriella anläggningar, samt andra näringsidkare att:

§ Delta i totalförsvarsplaneringen på begäran av en totalförsvarsmyndighet**§ Lämna de upplysningar om det egna företagets organisation och verksamhet som totalförsvarets myndigheter behöver för sin planering**

Dessutom reglerar lagen att den som i sin verksamhet – till följd av denna lag – får kännedom om interna förhållanden hos enskilda företag, inte obehörigen får röja eller utnyttja vad han fått veta. Samma gäller om man på grund av lagen får kännedom om förhållanden av betydelse för totalförsvaret eller för rikets säkerhet.

För elförsörjningen är även elberedskapslagen (1997:288), elberedskapsförordningen (1997:294) och Svenska Kraftnäts föreskrifter (SvKFS) utfärdade med stöd av elberedskapsförordningen tillämpliga.

SÄKERHETSSKYDDSLAGEN (1996:627)

Lagen innehåller bestämmelser om säkerhetsskydd hos staten, kommunerna och landstingen, bolag m. fl. som ägs eller styrs av dessa samt enskilda om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Här finns bestämmelser om säkerhetsskyddsåtgärder, säkerhetsskyddsavtal och registerkontroll.

SÄKERHETSSKYDDSFÖRORDNINGEN (1996:633)

Förordningen ger kompletterande bestämmelser till säkerhetsskyddslagen.

I förordningen behandlas bl. a. tillämpningsområden, definitioner, säkerhetsskyddschef, behörighet, informationssäkerhet och säkerhetsprövning.

LAG (1992:1403) OM TOTALFÖRSVAR OCH HÖJD BEREDSKAP

Lagen innehåller bestämmelser om totalförsvaret och anger vad som gäller vid höjd beredskap.

Totalförsvaret är verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar). För att stärka landets försvarsförmåga kan beredskapen höjas. Höjd beredskap är antingen skärpt beredskap eller högsta beredskap. Under högsta beredskap är totalförsvaret all samhällsverksamhet som då skall bedrivas.

FÖRORDNINGEN (2006:942) OM KRISBEREDSKAP OCH HÖJD BEREDSKAP

Bestämmelserna i denna förordning syftar till att statliga myndigheter genom sin verksamhet skall minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap.

Förordningen innehåller föreskrifter som dels reglerar krisberedskapen, dels ansluter till vad som föreskrivs i lagen (1992:1403) om totalförsvar och höjd beredskap.

LAG (2006:263) OM TRANSPORT AV FARLIGT GODS

Syftet med lagen är att förebygga, hindra och begränsa att transporter av farligt gods eller obehörigt förfarande med godset orsakar skador på liv, hälsa, miljö eller egendom.

Den som transporterar farligt gods eller lämnar farligt gods till någon annan för transport skall vidta de skyddsåtgärder och de försiktighetsmått i övrigt som behövs för att förebygga, hindra och begränsa att godset, genom transporten eller genom obehörigt förfarande med godset vid transport på land, orsakar sådana skador på liv, hälsa, miljö eller egendom som beror på godsets farliga egenskaper.

Farligt gods får transporteras endast på de villkor och under de förutsättningar som anges i denna lag och i de föreskrifter som har meddelats med stöd av lagen.

LAG (2007:1092) OM UPPHANDLING INOM OMRÅDENA VATTEN, ENERGI, TRANSPORTER OCH POSTTJÄNSTER

Denna lag tillämpas tillsammans med säkerhetskyddslagen vid de statliga och kommunala upphandlingar som rör rikets säkerhet. De företag som på uppdrag av ovanstående myndigheter utför sekretessbelagt arbete måste teckna särskilt säkerhetskyddsavtal.

För elförsörjningen har Svenska Kraftnät utgett föreskrifter och allmänna råd samt i samverkan med elbranschen ett antal vägledning (exempelvis Skyddsobjekt inom elförsörjningen, Fysiskt områdesskydd för elanläggningar, Fysiskt grundskydd, Säkerhetsanalys).

Föreskrifter och vägledning återfinns på Svenska Kraftnäts hemsida www.svk.se

Bilaga 2

BEFATTNINGSBESKRIVNING FÖR FÖRETAGETS SÄKERHETSFUNKTION

Denna bilaga utgör ett exempel på befattningsbeskrivning för företagets säkerhetsfunktion. Beroende på storlek på företag kan säkerhetsfunktionen bestå av en eller flera medarbetare.

Säkerhetschefen inom företaget ska ansvara för att aktivt driva säkerhetsarbetet och därigenom skydda medarbetare och entreprenörer, egendom, verksamhet och information.

Säkerhetschefen ska i säkerhetsfrågor ha en tydlig dubbelriktad kommunikation med VD, affärsområdeschefer, stabschefer, bolagschefer och eventuellt utsedda säkerhetsansvariga inom respektive enhet. I befattningen ingår även att tydligt samordna och stödja linjeverksamheten i frågor som avser säkerhet, säkerhetsskydd och beredskap.

Befattningen är i första hand strategisk och de operativa delarna hanteras av linjeorganisationen. Stor kännedom om företaget och dess verksamhet krävs. Funktionen är gemensam för hela företaget.

I uppdraget ingår även att säkerställa att rutiner övas.

EXEMPEL PÅ VERKSAMHETER DÄR SÄKERHET OCH BEREDSKAP ÄR VIKTIGT:

Produktion och distribution

Anläggnings- och leveranssäkerhet

Information och IT

Kontaktvägar i samband med inträffade störningar, mediakontakter, informationsklassning, dokumenthantering, besökssäkerhet m. m.

Personal

Rekrytering, utbildning m. m.

Fastigheter, lokaler

Tillträdesskydd, övervakning, brandskydd och utrymning

Miljö/Kvalitet

Nödlägesberedskap, verksamhetssystem, transporter av farligt gods, storskalig kemikaliehantering

SÄKERHETSFUNKTIONENS ARBETSUPPGIFTER KAN EXEMPELVIS VARA ATT:

- Rapportera och vara föredragande i säkerhetsfrågor i ledningsgrupper.
- Fortlöpande bedöma och värdera hot och risker mot företaget, informera samt föreslå åtgärder.
- Vara företagets försäkringsansvarige.
- Följa upp och utvärdera inträffade tillbud och incidenter samt föreslå förebyggande åtgärder och förbättringar av säkerhetsarbetet.

-
- Ansvara för att beredskapsplaner och säkerhetsskyddsinstruktioner tas fram, implementeras och revideras fortlöpande.
 - Vara rådgivare i säkerhetsfrågor och riskanalyser inom företaget.
 - Ansvara för att medarbetarna erbjuds säkerhetsutbildning, speciellt viktigt för nyanställda.
 - Planera och genomföra övningar för att öka beredskapen inför störningar.
 - Samverka med myndigheter och organ på lokal, regional och central nivå.
 - Aktivt informera sig om utvecklingen inom säkerhet och beredskap.
 - Ansvara för att företaget har ett fungerande systematiskt brandskyddsarbete, SBA.
 - Ansvara för att företaget har en rimlig informationssäkerhet.
 - Företräda företaget externt i säkerhetsrelaterade ärenden.
-

Bilaga 3

EXEMPEL PÅ SKYDDSVÄRDA UPPGIFTER

I denna bilaga redovisas exempel på skyddsvärda uppgifter som kan finnas inom företaget. Bilagan är uppdelad i två delar. Den första delen behandlar skyddsvärda uppgifter för företagets verksamhet och den andra delen behandlar skyddsvärda uppgifter med hänsyn till rikets säkerhet.

1. EXEMPEL PÅ SKYDDSVÄRDA UPPGIFTER FÖR FÖRETAGETS VERKSAMHET

Drift

Nätkartor, ritningar och övrig lägesbestämd information

Personal

Anställningsvillkor, löneuppgifter, omplacerings- och anpassningsärenden, personbedömningar, personuppgifter, sjukvårdsärenden, utvecklingssamtal

Planer

Affärsplaner, framtidsplaner, marknadsplaner, strukturplaner, utvecklingsplaner, bevakningsteknik, bevakningsplaner, marknads- och konkurrentanalyser, prognoser, skyddsåtgärder som vidtagits ur totalförvarssynpunkt

Priser

Anbud, budget, ekonomiska resultat, inköspriser, kostnads-kalkyler, offertpriser, provisioner, rabatter

Produktion

Inköpsinformation, kapacitet, reservanordningar, resurser, rutiner, tillverkningskostnader, bränsle- och magasinsvärden

Utveckling

Uppfinningar och patent, konstruktionsmetoder, spjutspets-teknologi

Övrigt

Brister och fel, dyrköpta erfarenheter, information om kunder och samarbetspartners, IT-system, IT-nätverk, andra kommunikationsnätverk, programvaror och backuprutiner, samverkansproblem, säkerhetssystem och lösenord, vissa anläggningars betydelse för elsystemet och totalförsvaret, vissa sammanställningar.

2. SKYDDSVÄRDA UPPGIFTER MED HÄNSYN TILL RIKETS SÄKERHET

I Svenska Kraftnäts *Vägledning Säkerhetsanalys* (www.svk.se) återfinns exempel på skyddsvärda uppgifter med hänsyn till rikets säkerhet. Dessa exempel är utformade i checklistor som redovisas för olika verksamhetstyper inom elförsörjningen.

Med skyddsvärda uppgifter med hänsyn till rikets säkerhet avses exempelvis:

- särskilt viktiga delar och anläggningar i elsystemet
- driftfunktioner och datastödssystem
- information om anläggningars svaga punkter
- anläggningars kapacitet, funktion och roll i elsystemet
- skyddsåtgärder som vidtagits
- exakta lägesangivningar för betydelsefulla anläggningar
- säkerhetsanalys

Bilaga 4

TYSTNADSFÖRBINDELSE

Denna bilaga kan användas som tystnadsförbindelse (mall) för såväl anställda som övrig personal (konsulter, praktikanter, entreprenörer med flera). För säkerhets-skyddad upphandling se även förslag i vägledning säkerhetskyddad upphandling på www.sakerhetspolisen.se/publicerat.

Namn:

Personnummer:

Denna dag har jag upplysts om den tystnadsplikt som gäller för mig under och efter min anställning/mitt uppdrag vid (företagets namn):

.....

Jag förbinder mig att under min anställning/mitt uppdrag vid företaget iaktta tystnadsplikt angående företagets affärsangelägenheter som är företagshemliga, sekretessbelagda personuppgifter samt sekretessbelagda uppgifter av totalförsvars-karaktär som jag får kännedom om under anställningen/uppdraget.

Överträdelse av tystnadsplikten kan medföra straffansvar och skadeståndsskyldig-het.

Jag är medveten om att tystnadsplikten gäller även efter avslutad anställning.

Datum: Namnteckning:

Namnförtydligande:

Bilaga 5

SEKRETESS- OCH SÄKERHETSAVTAL

AVTAL OM SEKRETESS OCH SÄKERHET (MALL)

Svensk Energi har genom EBITS tagit fram skiss på en avtalsmall för sekretess och säkerhet. Avtalsmallen avser att utgöra ett utkast till sekretessavtal. Utkastet måste inför att det ska användas i det särskilda fallet kompletteras alternativt revideras av den part som vill använda sig av det. De företag som önskar utgå från denna mall ska därför noggrant gå igenom avtalstexten och justera innehållet för att det ska fungera i det enskilda fallet. Avtalsmallen avser att vara en av i de flesta fall flera bilagor, som hänvisas från ett huvudavtal.

För säkerhetsskyddad upphandling se även förslag i vägledning säkerhetsskyddad upphandling på www.sakerhetspolisen.se/publicerat.

Bilaga xx: AVTAL OM SEKRETESS OCH SÄKERHET

Mellan parterna

BESTÄLLAREN:

och UTFÖRAREN:

.....
Beställaren

.....
Utföraren

.....
Adress

.....
Adress

.....
Postnummer och ort

.....
Postnummer och ort

.....
Organisationsnummer

.....
Organisationsnummer

(nedan kallat BESTÄLLAREN)

(nedan kallat UTFÖRAREN)

har denna dag träffats följande avtal, nedan kallat AVTALET.

1. Allmänt

UTFÖRAREN kommer att utföra visst arbete/uppdrag för BESTÄLLAREN. I genomförandet av sitt uppdrag kan UTFÖRAREN komma att, som en del av sitt uppdrag eller eljest, erhålla information om BESTÄLLAREN eller BESTÄLLARENS samarbetspartners som BESTÄLLAREN önskar/är skyldigt att inte sprida. Sådan information kan, p.g.a. AVTALET, annat avtal eller lag eller annan författning bestå av eller innehålla delar som inte får utnyttjas eller röjas. UTFÖRAREN skall alltid upprätthålla minst de i AVTALET angivna reglerna. Annat avtal kan komma att tecknas gällande utökad sekretess, säkerhet och/eller andra frågor med bärighet härpå, om så skulle vara motiverat. UTFÖRAREN skall alltid, utöver AVTALET, beakta och följa BESTÄLLARENS vid varje tid gällande policier, föreskrifter och regelverk, se bilaga nr xx.

2. Åtagande om sekretess

UTFÖRAREN förbinder sig att, utan begränsning i tiden, inte för tredje man avslöja konfidentiell information, vilken UTFÖRAREN erhåller från BESTÄLLAREN eller i övrigt får kännedom om i samband med genomförande av arbete/uppdrag för BESTÄLLAREN.

Med "konfidentiell information" avses i AVTALET varje upplysning – av teknisk, kommersiell eller annan art – oavsett om upplysningen dokumenterats eller icke, med undantag för:

- a) upplysning, som är allmänt känd eller kommer till allmän kännedom på annat sätt än genom brott från UTFÖRARENS sida mot innehållet i AVTALET.
- b) upplysning, som UTFÖRAREN kan visa att UTFÖRAREN redan kände till innan den mottogs från BESTÄLLAREN eller i samband med utförande av arbete/uppdrag för BESTÄLLAREN kom till UTFÖRARENS kännedom från annan källa än BESTÄLLAREN.
- c) upplysning, som UTFÖRAREN mottagit från tredje man utan att vara bunden av sekretessplikt i förhållande till denne.

I fall som avses under c) ovan har dock UTFÖRAREN inte rätt att avslöja för utomstående att samma upplysning även mottagits från BESTÄLLAREN eller vid utförande av arbete/uppdrag enligt AVTALET.

3. Personal och underentreprenörer

UTFÖRAREN förbinder sig att tillse att UTFÖRARENS anställda inte till utomstående vidarebefordrar konfidentiell information. Det åligger därvid UTFÖRAREN att tillse att de anställda som kan antas komma i kontakt med information av konfidentiell natur är bundna att hemlighålla denna information i samma utsträckning som UTFÖRAREN enligt AVTALET.

UTFÖRAREN skall, innan enskild person avdelas för arbete/uppdrag för BESTÄLLAREN, ha genomfört personbedömning innefattande bl. a. vederbörandes pålitlighet med beställaren samt – om anledning härtill uppkommit vid personbedömningen – samråda med BESTÄLLAREN.

UTFÖRAREN ansvarar för att dess anställda genom UTFÖRARENS försorg erhållit erforderlig information och adekvat utbildning gällande dels de hot och risker som kan förekomma i aktuellt avseende inom BESTÄLLARENS verksamhet, dels de säkerhets- skyddsåtgärder som följer av policier, föreskrifter och regelverk som BESTÄLLAREN vid vart tillfälle tillämpar. Om UTFÖRAREN så begär, lämnar BESTÄLLAREN uppgift och information i dessa frågor.

Vad i föregående stycken angetts om anställda gäller även av UTFÖRAREN anlidade underentreprenörer, konsulter o. dyl.

4. Användning av konfidentiell information

UTFÖRAREN får endast använda konfidentiell information, som tillhandahållits av BESTÄLLAREN, för de ändamål som särskilt anges i huvudavtalet med tillhörande bilagor.

Konfidentiell information som UTFÖRAREN fått åtkomst till under genomförande av arbete/uppdrag för BESTÄLLAREN, men som inte lämnats till UTFÖRAREN eller UTFÖRAREN annars borde ha förstått inte varit avsedd att komma till UTFÖRARENS kännedom, får aldrig användas av UTFÖRAREN. Utöver vad som nedan stadgas om återlämnande av information gäller, i fall som anges i detta stycke, att UTFÖRAREN skall tillse att fullständigt till BESTÄLLAREN redovisa alla omständigheter som kan ha relevans för BESTÄLLARENS utredning gällande UTFÖRARENS åtkomst och hantering av den i detta avseende relevanta konfidentiella informationen.

5. Särskilt gällande säkerhet och återlämnande av information m. m.

UTFÖRAREN skall, på begäran från BESTÄLLAREN och i vart fall i samband med att arbetet/uppdraget för BESTÄLLAREN avslutas, till BESTÄLLAREN återlämna alla dokument och göra andra informationsbärare av konfidentiell information som är i UTFÖRARENS besittning oläsliga och ej möjliga att återskapa.

UTFÖRAREN ansvarar för att mottagandet av konfidentiell information vederbörligen kvitteras och för att kopiering av sådan information ej sker utan BESTÄLLARENS i förväg lämnade skriftliga tillstånd.

UTFÖRAREN ansvarar för, och är skyldigt att ha rutiner som säkerställer, att all konfidentiell information som hanteras under UTFÖRARENS arbete/uppdrag – gällande såväl vid lagring som transport – är skyddad från åtkomst av obehörig.

6. Myndighets rätt till information

UTFÖRARENS ansvar och åtaganden enligt AVTALET hindrar inte UTFÖRAREN från att till myndighet lämna ut sådana uppgifter som efterfrågas av myndigheten med stöd av lag eller annan författning.

7. Skadestånd

Part skall ersätta motparten den skada denne lider genom brott mot AVTALET. Skadeståndet skall motsvara den verkliga skadan alternativt begränsas till xx basbelopp. Ersättning för ren förmögenhetsskada utgår inte.

8. Rubriker

Indelningen av AVTALET i olika avsnitt och åsättande av rubriker skall inte påverka AVTALETs tolkning.

9. Giltighet och UTFÖRARENS informationsplikt m. m.

UTFÖRAREN är bundet av AVTALET fr. o. m. undertecknandet. AVTALET gäller under den tid arbete/uppdrag utförs av UTFÖRAREN, dock i vissa delar – t. ex. sekretess – även därefter.

Skulle UTFÖRAREN inse, eller ha befogad anledning att anta, förekomst av eller ändring i förhållanden som har betydelse för säkerhets- och/eller sekretessfrågor, skall UTFÖRAREN omedelbart informera BESTÄLLAREN därom.

Oavsett föregående stycke skall BESTÄLLAREN, i eget val och omgående efter framställd begäran därom, av UTFÖRAREN lämnas tillfälle att företa inspektion och/eller revision av UTFÖRARENS uppfyllande av sina förpliktelser enligt AVTALET.

Vad i föregående stycken sagts gäller bl. a., dock inte begränsat till, vid ny ägares förvärv av hela eller delar av UTFÖRAREN.

10. Bestämmelses ogiltighet

Skulle någon bestämmelse i AVTALET eller del därav befinnas ogiltig, skall detta inte innebära att AVTALET i dess helhet är ogiltigt utan skall, i den mån ogiltigheten väsentligen påverkar parts åtagande eller förpliktelse enligt AVTALET, skälig jämkning i AVTALET ske.

11. Passivitet

Parts underlåtenhet att utnyttja någon rättighet enligt AVTALET eller underlåtenhet att påtala visst förhållande hänförligt till AVTALET skall inte innebära att part frånfallit sin rätt i sådant avseende.

Skulle part vilja avstå från att utnyttja viss rättighet eller att påtala visst förhållande skall sådant avstående ske skriftligen i varje enskilt fall.

12. Skiljedom

Tvist i anledning av AVTALET får inte hänskjutas till domstol utan skall avgöras av skiljenämnd enligt vid påkallandet gällande lag om skiljeförfarande. Parterna skall stå för sina egna kostnader och dela lika på kostnader för skiljemännens arbete och utlägg.

Skiljeförfarandet skall äga rum i X-stad. Svensk rätt skall tillämpas.

AVTALET har upprättats i två original exemplar och utväxlats mellan parterna.

.....
Ort och datum

.....
Ort och datum

.....
Beställaren

.....
Utföraren

.....
Namnteckning firmatecknare, beställaren

.....
Namnteckning firmatecknare, utföraren

.....
Namnförtydligande

.....
Namnförtydligande

Bilaga 6

PERSONALHANTERING ANSTÄLLDA

Denna bilaga anger exempel på åtgärder, sett ur säkerhetssynpunkt, angående personalhanterings olika skeden för anställd arbetstagare. Med anställd avses här arbetstagare med anställningsformen tillsvidareanställning, visstidsanställning, provanställning eller motsvarande.

Före annonsering:

- Anställningens betydelse för företaget. Är det en nyckelpersonsbefattning?
- Är eller bör anställningen vara säkerhetsklassad?

Före anställning:

För att kunna göra en rättvisande personbedömning bör bland annat följande frågeställningar belysas avseende personen som ska rekryteras:

- Tidigare anställningar (helst 10 år tillbaka)
- Utbildningar
- Andra referenser
- Familjeförhållanden
- Intressen
- Personliga förhållanden och vanor (ekonomi, alkohol och narkotika)

Med nuvarande lagstiftning kan inhämtning av öppen information inhämtas via någon eller några av följande källor:

- Statens personadressregister SPAR (mantalsskrivningsort, make/maka, barn, personnummer)
- Centrala bilregistret rörande fordon och körkortsinnehav
- Skatteverket rörande inkomster, förmögenheter och avdrag
- Centralnämnden för fastighetsdata för uppgift om fastighetsinnehav
- Bolagsverket rörande ägarförhållande i bolag
- Kreditupplysningsföretag (vissa uppgifter är upp till ett år gamla) för uppgifter om kreditvärdighet, betalningsanmärkningar, omfrågningar, styrelseuppdrag i företag m. m.

Obs! Vid begäran om upplysning från kreditupplysningsföretag lämnas alltid en kopia till den omfrågade med uppgift om vem som frågat.

- Skolor, institutioner och företag där den aktuella personen tidigare studerat eller arbetat.

I samband med anställningsintervjun bör företaget informera om följande:

- Introduktion om företaget och dess policy, den egna enhetens uppgifter och organisation, planerade arbetsuppgifter och befogenheter, tystnadsplikt och tystnadsförbindelse (undvik att ge företagshemlig information)
- Alkohol- och drogpolicy
- Etiska regler inom företaget
- Registerkontroll vid säkerhetsklassad tjänst. Se kapitel 8.

Vid anställningens början:

- Tystnadsförbindelse (senast vid formell anställning). Se separat bilaga
- Fördjupad introduktion och utbildning avseende företaget och dess policy, den egna enhetens uppgifter och organisation, egna arbetsuppgifter och befogenheter.
- Säkerhetspolicy
- Behovsanpassad säkerhetsutbildning/information
- Etiska regler inom företaget

Under anställningstiden sker kontinuerlig uppföljning:

- Av personliga förhållanden
- Av den anställdes lojalitet och förhållande till arbete, kollegor och samarbetspartner

Vid byte av tjänst inom företaget bör liknande åtgärder vidtas som vid nyanställning.

Vid anställningens upphörande bör följande klarläggas:

- Varför vederbörande slutar
- Hos vem nyanställning sker
- Behov av ändrade arbetsuppgifter under uppsägningstiden (karantän)
- Behov av att reducera tillgång på informationssystem
- Att vederbörande inte har rätt att ta med sig information från hemkatalog, hårddiskar, projektdokument m. m.
- Vederbörandes unika och därmed för företaget betydelsefulla kunskap
- Tystnadspliktens innebörd

När anställningen upphör ska omgående:

- All företagshemlig och företagsintern information återlämnas
- Alla behörigheter, nycklar och ID-kort dras in
- Företagets kredit- och betalkort återlämnas
- Koder som vederbörande haft tillgång till ändras
- Övrig av företaget tillhandahållen materiel och utrustning återlämnas

Bilaga 7

PERSONALHANTERING

ÖVRIG PERSONAL

Denna bilaga anger exempel på åtgärder, sett ur säkerhetssynpunkt, angående personalhanterings olika skeden för övrig personal. Med övrig personal avses här exempelvis entreprenörer, konsulter, praktikanter, examensarbetare eller forskare.

För att skydda företagets information och kunskap ges nedan exempel på åtgärder som kan vidtas.

Före uppdragets början:

- Orientera egen säkerhetschef (säkerhetsansvarig) i tidigt skede
- Utse en kontaktman eller handläggare/fadder i förekommande fall
- Klara ut försäkringsförhållanden
- Klara ut ägarförhållande till utfört arbete

Allmänna uppgifter rörande företag och personer

Med nuvarande lagstiftning kan inhämtning av öppen information ske via:

- Statens personadressregister SPAR (mantalsskrivningsort, make/maka, barn, personnummer)
- Centrala bilregistret rörande fordon och körkortsinnehav
- Skatteverket rörande inkomster, förmögenheter och avdrag
- Centralnämnden för fastighetsdata för uppgift om fastighetsinnehav
- Bolagsverket rörande ägarförhållande i bolag
- Kreditupplysningsföretag (vissa uppgifter är upp till ett år gamla) för uppgifter om kreditvärdighet, betalningsanmärkningar, omfrågningar, styrelseuppdrag i företag m. m.

Obs! Vid begäran om upplysning från kreditupplysningsföretag lämnas alltid en kopia till den omfrågade med uppgift om vem som frågat.

- Skolor, institutioner och företag där den aktuella personen tidigare studerat eller arbetat.

Om uppdraget innebär kontakt med företagshemlig information ska ett sekretess- och säkerhetsavtal upprättas. Se exempel i bilaga. Den bör bland annat innehålla:

- Förteckning över personal som får utföra uppdraget
- Regler för hantering av företagshemlig information
- Krav på legitimationshandling
- Bestämmelser för tillträde och fotografering
- Tystnadsförbindelse; se separat bilaga

Fastställt avtal ska delges berörda och uppdragsgivaren ska säkerställa att uppdraget är känt och accepterat.

Under uppdraget:

- Följ upp att avtal och andra bestämmelser för säkerhetsskyddet efterlevs
- Orientera egen säkerhetschef om avvikelser och incidenter

Efter uppdraget:

- Påminna om träffad tystnadsförbindelse
- Återkalla behörigheter och meddela övriga berörda att uppdraget avslutats
- Återkräva utlämnad företagshemlig information

Bilaga 8

ÅTGÄRDER VID BOMBHOT

Syftet med denna bilaga är att ge kunskap kring vad man bör tänka på under ett hot samt vad som är viktigt att observera. Checklistan är därför lämplig att använda vid utbildningssammanhang. Den kan även med fördel användas efter ett genomfört hot för att på så vis utgöra vägledning för fortsatt hantering. Det är viktigt att utan dröjsmål rapportera om det inträffade samt låta polis värdera situationen. Utrymning är en annan viktig faktor som måste beaktas. Det är en fördel om det på företaget finns utrustning för att spela in inkomna hotsamtal. Detta underlättar polisens fortsatta arbete.

En kopia av checklistan bör finnas tillgänglig i exempelvis driftcentral, kundtjänst, växel eller reception.

DÅ NÅGON MEDDELAR ETT BOMBHOT PER TELEFON:

Var lugn. Var vänlig. Avbryt inte. Försök bibehålla samtalet. Starta om möjligt inspelning. Försök spåra samtalet. Anteckna dag och exakt tidpunkt.

Frågor:

1. När ska bomben explodera?
2. Var har bomben placerats?
3. När placerades bomben ut?
4. Hur ser bomben ut?
5. Vilken sorts bomb är det?
6. Vad får bomben att explodera?
7. Har du placerat ut bomben själv?
8. Varför har bomben placerats ut?
9. Vad heter du?
10. Var finns du nu?

HUR LÖD HOTET EXAKT?

Åtgärder:

Ditt namn:

Säkerhetsansvarig kontaktad kl

Beslut om utrymning av lokalerna kl / genomfört kl

Polisen larmad kl

Bombhotarens identitet:

- Man Kvinna Pojke Flicka

Bombhotarens röst:

- Högljudd Tystlåten Mörk Ljus
 Sluddrig Mjuk/behaglig

Bombhotarens tal:

- Snabbt Distinkt Långsamt Välståndat
 Stammande Svordomar Läspande Förvrängt
 Fackuttryck Dialekt Utländsk brytning

Bombhotarens attityd:

- Lugn Upphetsad Förtrogen med företaget

Bakgrundsljud:

- Maskiner Gatuljud Flygplan
 Röster Musik Högtalarutrop
 Blandat Annat:

Bilaga 9

CHECKLISTA INFORMATIONSSÄKERHET VID HANTERING AV IT-SYSTEM

SÄKERHET FÖR DEN PRIVATE HEM-PC-ANVÄNDAREN OCH DET MINDRE ENERGIFÖRETAGET

Observera att bristande säkerhet i PC:n inte bara drabbar dig själv, det är också ett potentiellt hot för alla andra Internetanslutna datorer världen över.

En dator som är ansluten till Internet har en del krav att leva upp till. Stämmer påståendena för dig själv?

	Ja	Nej
1. Datorn säkerhetsuppdateras kontinuerligt (patchar för t. ex. Windows och program läggs in).	<input type="checkbox"/>	<input type="checkbox"/>
2. Programvara för skydd mot skadlig kod är uppdaterad.	<input type="checkbox"/>	<input type="checkbox"/>
3. Antivirusprogrammet är uppdaterat.	<input type="checkbox"/>	<input type="checkbox"/>
4. Stor försiktighet (på gränsen till paranoid inställning) råder vid användningen av datorn vid besök på Internet för att bland annat begränsa möjligheten till att lösenord eller kontokortsnummer stjäls.	<input type="checkbox"/>	<input type="checkbox"/>

För din egen skull är det också av värde att administrationen av systemet fungerar (t. ex. backup av data och defragmentering av hårddisken).

Checklistan nedan har till syfte att komplettera de råd som givits ovan. Syftet att stärka det mindre företaget i sin strävan att nå upp till sin ambitionsnivå för informations- och IT-säkerhet. När du satt kryss i ja- och nej-rutorna gör du lämpligen en åtgärdslista för att ta hand om "nej-svaren".

Sist i dokumentet har en liten ordlista infogats för att belysa en del termer.

I texten förekommer "<org>" eller "<org:s>". Ersätt detta med namnet på det egna energiföretaget.

KLASSIFICERING AV TILLGÅNGAR

Förteckning över skyddsvärda tillgångar	Noteringar
<p>De skyddsvärda tillgångarna ska vara förtecknade och märkta. Med förteckning avses även elektroniskt register. Av förteckningen ska fabrikat, produkt och version framgå. IT-systemets informationstillgångar ska vara inventerade och bedömda m.a.p. sekretess. Med informationstillgångar avses t. ex. ritningar, mönster, strukturer, beskrivningar av sammanhang, m. m. Informationstillgångarna är av större värde än vad man först kan tro. Gör gärna en grov bedömning av hur lång tid det har tagit att skapa denna information. Vad är den värd? Om värdet är känt bidrar det till att bedöma behovet av sekretess.</p>	
Ja Nej	
Det finns en förteckning över maskinvaror <input type="checkbox"/> <input type="checkbox"/>	
Det finns en förteckning över programvaror <input type="checkbox"/> <input type="checkbox"/>	
Det finns en förteckning över skyddsvärda informationstillgångar <input type="checkbox"/> <input type="checkbox"/>	
Informationstillgångarna är bedömda i avseende på sekretess <input type="checkbox"/> <input type="checkbox"/>	

PERSONAL OCH SÄKERHET

Säkerhet i beskrivning av ansvar i arbetet	Noteringar
<p>De krav som gäller för användare ska vara definierade av systemägaren.</p>	
<p>Kraven ska avse såväl säkerhet som kompetens och ska vara dokumenterade och kommunicerade.</p>	
Ja Nej	
Systemägaren har formulerat vilka krav som ställs på användare <input type="checkbox"/> <input type="checkbox"/>	
Utbildning och övning i informationssäkerhet	Noteringar
<p>Användare av IT-system ska ha fått nödvändig utbildning, och utbildningen ska ha omfattat både IT-systemets användning och säkerhet.</p>	
Ja Nej	
Användarna har fått utbildning i systemets användning och säkerhet <input type="checkbox"/> <input type="checkbox"/>	
Användardokumentation	Noteringar
<p>Användardokumentation för alla användare av system och applikation ska finnas och ska vara tillgängliga.</p>	
Ja Nej	
Handböcker och/eller lathundar finns som beskriver användningen <input type="checkbox"/> <input type="checkbox"/>	

Forts. "Personal och säkerhet"

<p>Rapportering av säkerhetsincidenter</p> <p>Rutin för rapportering och uppföljning av incidenter ska finnas och följas. Rutinen ska omfatta hur information ska förmedlas, till vem rapportering ska ske och hur information sammanställs. Incidenterna ska sedan följas upp, dvs. de brister i organisationen som lett till att incidenten inträffat måste rättas till.</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns en rutin för rapportering av incidenter <input type="checkbox"/> <input type="checkbox"/></p> <p>Rutinen för rapportering av incidenter följs <input type="checkbox"/> <input type="checkbox"/></p> <p>Uppföljning av rapporterade incidenter görs för att rätta till eventuella brister i organisationen (t. ex. brister i rutiner) <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Rapportering av funktionsfel och brister</p> <p>Rutin för rapportering av fel, säkerhetsmässiga svagheter, brister och ändringsförslag ska finnas.</p> <p>I rutinen ska det vara fastställt till vem och hur rapportering ska ske.</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns en rutin för rapportering av funktionsfel och upptäckta svagheter i säkerheten <input type="checkbox"/> <input type="checkbox"/></p> <p>Rutinen för rapportering av fel och säkerhetsmässiga svagheter följs <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

FYSISK OCH MILJÖRELATERAD SÄKERHET

<p>Skalskydd</p> <p>Skalskydd för de serverdatorer som ingår i IT-systemet ska anordnas enligt <org:s> anvisningar för skalskydd.</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns anvisningar för skalskydd <input type="checkbox"/> <input type="checkbox"/></p> <p>Serverdatorerna har installerats enligt anvisningarna för skalskydd <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Elförsörjning</p> <p>Elmiljö för serverdator ska vara säkerställd med t. ex. avbrottsfri kraft i de fall där tillgängligheten kräver detta.</p> <p style="text-align: right;">Ja Nej</p> <p>Elförsörjningen för serverdatorerna är tillfredsställande <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

Forts. "Fysisk och miljörelaterad säkerhet"

Underhåll av utrustning	Noteringar
<p>Samtliga underhållsavtal som har betydelse för systemet ska vara förtecknade och de ska bevakas kontinuerligt. Syftet är att se till att enskilda avtal har rätt nivå och att endast relevanta avtal är gällande (dvs. inga avtal på ut-rangerade produkter).</p> <p>Leverantörens rekommenderade underhållsplan för ut-rustningen ska följas.</p>	
Ja Nej	
<p>Alla viktiga underhållsavtal med leverantörer finns förtecknade</p>	<input type="checkbox"/> <input type="checkbox"/>
<p>Underhållsavtalen bevakas kontinuerligt (rätt nivå, ej pensionerad utr.)</p>	<input type="checkbox"/> <input type="checkbox"/>
<p>I de fall leverantören har rekommenderad underhållsplan, följs den</p>	<input type="checkbox"/> <input type="checkbox"/>

STYRNING AV KOMMUNIKATION OCH DRIFT

Drifrutiner och driftansvar	Noteringar
<p>Verksamheten ställer vissa krav på systemen att uppfylla. Exempel på sådana krav är: säkerhetskrav, tillgänglighetskrav och organisatoriska krav (t. ex. bemanning). Flertalet av dessa krav bör finnas nedtecknade och berörd personal måste känna till dem. I medelstora och större företag brukar den här typen av krav finnas nedtecknade i något som kallas SLA (Service Level Agreement).</p>	
Ja Nej	
<p>De krav som verksamheten ställer på systemet finns nedtecknade</p>	<input type="checkbox"/> <input type="checkbox"/>
<p>Kraven är kända av den personal som berörs</p>	<input type="checkbox"/> <input type="checkbox"/>
Säkerställda resurser	Noteringar
<p>Det är viktigt att personalen vet vad den ska göra när en situation inträffar som hotar verksamheten. Men det är också viktigt att resurser ställs till förfogande i tillräcklig utsträckning för att klara av den uppkomna situationen.</p> <p>I medelstora och större företag brukar det finnas en delegeringsordning som reglerar det här.</p>	
Ja Nej	
<p>Det finns beskrivet hur personalresurser omfördelas vid extraordinära händelser, t. ex. incidentberedskap</p>	<input type="checkbox"/> <input type="checkbox"/>
<p>Det finns beskrivet hur extra personal kallas in vid viss typ av händelse, t. ex. incident</p>	<input type="checkbox"/> <input type="checkbox"/>
<p>Det finns beskrivet hur prioritering görs mellan olika system i händelse av incident</p>	<input type="checkbox"/> <input type="checkbox"/>

Forts. "Styrning av kommunikation och drift"

<p>Styrning av ändringar i drift</p> <p>Det har visat att störningar i IT-drift i hög grad beror på att någon gjort en förändring utan att vara fullständigt insatt i konsekvenserna. Ett visst mått av byråkrati brukar därför betala sig väl för att öka kvaliteten i förändringen.</p> <p>Vid större förändringar är det av värde att ett systemgodkännande ges av en person i lämplig ansvarsposition, t. ex. den som är ansvarig för IT-driften. Begreppet systemgodkännande behandlas mer utförligt nedan.</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns en formell rutin för ändringshantering <input type="checkbox"/> <input type="checkbox"/></p> <p>Rutinen för ändringshantering är en del av IT-systemets förvaltningsrutiner <input type="checkbox"/> <input type="checkbox"/></p> <p>Rutinen för ändringshantering inbegriper systemgodkännande <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Hantering av säkerhetsincidenter</p> <p>Att hantera en allvarlig IT-incident kräver något extra av personalen. Kanske driften står still och verksamheten är lamslagen. Det måste då finnas resurser och dessa måste vara organiserade enligt ett på förhand fastställt sätt. Eftersom kaos antagligen råder kan situationen endast bemästras om personalen tränats för detta i förväg.</p> <p>(Jämför med "3.3.1 Rapportering av säkerhetsincidenter" som endast avser rapportering och uppföljning av incidenter)</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns en plan för hur personalen omgrupperas för att hantera en allvarlig IT-incident <input type="checkbox"/> <input type="checkbox"/></p> <p>Personalen har tränats för att hantera allvarliga IT-incidenter <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Kapacitetsplanering</p> <p>Kapaciteten i IT-systemet brukar vara något som ständigt behöver bevakas eftersom mängden data som ska hanteras ökar hela tiden. Det krävs därför att prognoser görs regelbundet för tillräcklig framförhållning.</p> <p>Exempel på systemresurser som måste övervakas och göras en prognos för är processorkraft, diskutrymme och bandbredd för kommunikationslänkar.</p> <p style="text-align: right;">Ja Nej</p> <p>Systemresurserna övervakas ständigt och kapacitetsprognoser görs <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

Forts. "Styrning av kommunikation och drift"

<p>Systemgodkännande</p> <p>Driftsättning av IT-system visar sig ofta ske lite väl lättvindigt vilket skapar både irritation och extra kostnader i verksamheten. Ett driftsatt system där utvecklingspersonalen gör ständiga "fixar" med avbrott för produktionen är ett tecken på att systemet ej är färdigutvecklat och ej heller tillräckligt testat.</p> <p>En driftsättningsrutin är till god hjälp. Syftet med en sådan rutin är att det ska ske en kontrollerad, protokollförd överlämning av IT-systemet från utvecklingspersonalen till driftorganisationen. En sådan överlämning ska föregås av en acceptanstest.</p> <p style="text-align: right;">Ja Nej</p> <p>Det finns en dokumenterad driftsättningsrutin för IT-system <input type="checkbox"/> <input type="checkbox"/></p> <p>Rutinen följs vid driftsättning och protokoll upprättas <input type="checkbox"/> <input type="checkbox"/></p> <p>Innan driftsättning görs en acceptanstest <input type="checkbox"/> <input type="checkbox"/></p> <p>Driftsättningsrutinen används även vid förändringar i IT-systemet <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Systemdokumentation</p> <p>De alltmer komplexa IT-systemen gör det svårt för ny personal att sätta sig in i hur de fungerar, något som är förödande vid konfigurationsändringar eller andra typer av förändringar. Med systemdokumentation av tillräcklig kvalitet underlättas det för ny personal att sätta sig in i vad som händer "under huven". Sådan dokumentation ska uppdateras vid varje större uppdatering av systemet.</p> <p style="text-align: right;">Ja Nej</p> <p>Alla viktiga IT-system har systemdokumentation som tillräckligt väl beskriver hur de fungerar och hur de ska underhållas <input type="checkbox"/> <input type="checkbox"/></p> <p>Personalen har tränats för att hantera allvarliga IT-incidenter <input type="checkbox"/> <input type="checkbox"/></p> <p>Systemdokumentationerna hålls kontinuerligt uppdaterade <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Driftdokumentation</p> <p>De alltmer komplexa IT-systemen kräver att det finns dokumentation som beskriver den dagliga driften av systemet.</p> <p>Driftdokumentation (ej att förväxla med handhavandokumentation för användarna) av tillräcklig kvalitet är en förutsättning för upprätthållandet av tillgängligheten.</p> <p style="text-align: right;">Ja Nej</p> <p>Alla viktiga IT-system har driftdokumentation som tillräckligt väl beskriver vad driftpersonalen ska tänka på <input type="checkbox"/> <input type="checkbox"/></p> <p>Dessa dokument är granskade och godkända vid driftöverlämning <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

Forts. "Styrning av kommunikation och drift"

<p>Åtgärder mot otillförlitliga program</p> <p>De PC-miljöer där användarna själva kan installera sina favoritprogram skapar onödigt mycket trassel med åtföljande kostnader. En tydlig trend sedan många år tillbaka är att endast sådana program som godkänts formellt inom företaget får finnas i PC-miljö. Det blir också allt vanligare att enskilda användare ej ges behörighet att installera program själva.</p> <p style="text-align: right;">Ja Nej</p> <p>PC-miljön är av typen "standardarbetsplats" och användaren ges inte behörighet att installera egna program <input type="checkbox"/> <input type="checkbox"/></p> <p>De program som installeras i PC utöver standardutbudet har inom företaget testats och godkänts <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Säkerhetskopiering</p> <p>Säkerhetskopieringen är den livlina som aldrig får brista eftersom informationen är företagets viktigaste resurs. Brister i säkerhetskopieringen kan vid dataförlust åsamka företaget oerhörd skada. Även förlusten av till synes ganska oviktig information är till men för verksamheten.</p> <p style="text-align: right;">Ja Nej</p> <p>All data säkerhetskopieras varje dygn <input type="checkbox"/> <input type="checkbox"/></p> <p>Av märkningen på säkerhetskopian går det att härleda den till en given systemkonfiguration (inkl. versioner på maskinvara och aktuella programvaror) <input type="checkbox"/> <input type="checkbox"/></p> <p>Säkerhetskopiorna förvaras på betryggande sätt i företagets lokaler <input type="checkbox"/> <input type="checkbox"/></p> <p>En ytterligare omgång säkerhetskopior förvaras på ett betryggande avstånd från företagets lokaler m.a.p. brandrisken <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Utbyte av information mellan system</p> <p>IT-systemen är idag mer eller mindre sammankopplade med andra system inom eller utanför företaget. Ett antal beroenden mellan systemet och andra system har på så vis skapats och dessa beroenden måste finnas dokumenterade.</p> <p style="text-align: right;">Ja Nej</p> <p>För varje system hos företaget är det klarlagt vilka andra system som är beroende av systemet och på vad sätt <input type="checkbox"/> <input type="checkbox"/></p> <p>För varje system hos företaget är det klarlagt på vad sätt det är beroende av andra system <input type="checkbox"/> <input type="checkbox"/></p> <p>I de beroenden som identifierats finns det klarlagt vilka krav på riktighet och tillgänglighet som råder <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

Forts. "Styrning av kommunikation och drift"

<p>Att tänka på för system som publicerar information på Internet</p> <p>Det ställs vissa speciella krav på system som används för att publicera information på Internet.</p> <p style="text-align: right;">Ja Nej</p> <p>En formell rutin för godkännande av informationen innan den publiceras på Internet <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
--	--------------------------

STYRNING AV ÅTKOMST

<p>Krav som ställs på användare av system</p> <p>I samband med att ett system tas i drift är det viktigt att det fastställs vad som gäller för användarna.</p> <p style="text-align: right;">Ja Nej</p> <p>För varje enskilt system har det identifierats vilka användare som ska få tillgång till systemet och dess information <input type="checkbox"/> <input type="checkbox"/></p> <p>För varje enskilt system har det identifierats vilka krav som gäller för de användare som tilldelats behörighet (behörighetsprofil) <input type="checkbox"/> <input type="checkbox"/></p> <p>För varje enskilt system har det identifierats vad som gäller för användarens arbetsplatsutrustning <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Krav på system som är åtkomligt från Internet</p> <p>Då system ska nås från Internet gäller att man sätter sig in i hur målgruppen ser ut som ska nå informationen.</p> <p style="text-align: right;">Ja Nej</p> <p>För varje enskilt system som kan nås från Internet har det klarlagts vilka som får behörighet till informationen <input type="checkbox"/> <input type="checkbox"/></p> <p>För varje enskilt system som kan nås från Internet har det klarlagts vilken behörighetsprofil som ska gälla <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Användarregistrering</p> <p>Att släppa in användare i ett system kräver att behörighetsprofilen för varje enskild användare är noga genomtänkt, dvs. ej mer behörighet än vad som verkligen erfordras för att användaren ska kunna sköta sitt jobb.</p> <p style="text-align: right;">Ja Nej</p> <p>För varje enskilt system finns det rutiner för hur behörighet delas ut <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

KONTINUITETSPLANERING

<p>Informera användare då t ex system tas ned</p> <p>Användarna måste få bli förvarnade i tid innan systemet tas ned för service. Det är också viktigt att informera om att tidigare, besvärande fel äntligen har åtgärdats och driften åter flyter på.</p> <p style="text-align: right;">Ja Nej</p> <p>En rutin finns för att informera användare av ett givet systemet om att det kommer att tas ned för service en viss tid <input type="checkbox"/> <input type="checkbox"/></p> <p>Om andra system berörs av att systemet tas ned, ska rutinen omfatta information även till dessa personer. Rutinen klarar detta. <input type="checkbox"/> <input type="checkbox"/></p> <p>En rutin finns för att informera användare om att ett fel som besvärat dem har rättats till <input type="checkbox"/> <input type="checkbox"/></p> <p>Om andra system berörs av felrättningen ska rutinen omfatta information även till dessa personer. Rutinen klarar detta. <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Bedöma konsekvenser av allvarliga avbrott</p> <p>Riskanalysen är det enskilt viktigaste instrumentet för att komma tillrätta med svagheter och potentiella hot både organisatoriskt och tekniskt. Genom ständigt återkommande riskanalyser kan företaget agera proaktivt, dvs. förbereda sig så gott det går för störningar i verksamheten.</p> <p>Riskanalys görs förslagsvis för att bedöma konsekvenserna av allvarliga avbrott och resultaten från riskanalyserna kan tjäna som underlag för kontinuitetsplaneringen (se nedan).</p> <p style="text-align: right;">Ja Nej</p> <p>Metod för riskanalys finns inarbetad på företaget <input type="checkbox"/> <input type="checkbox"/></p> <p>Metoden för riskanalys används regelbundet för att identifiera potentiella hot, både organisatoriska och tekniska <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

Forts. "Kontinuitetsplanering"

<p>Kontinuitetsplaner och reservrutiner</p> <p>Kontinuitetsplanerna är de livlinor som gör att företaget överlever mycket allvarliga störningar, dvs. kontinuiteten i verksamheten upprätthålls även om "det värsta tänkbara" inträffar. Kontinuitetsplanerna kallas därför ibland för katastrofplaner. Det är med hjälp av resultat från riskanalyser som kontinuitetsplanerna utarbetas.</p> <p>Observera att kontinuitetsplaner måste testas så verklig-hetstroget som möjligt för att det ska gå att lita på dem.</p> <p>Det finns två typer av kontinuitetsplaner:</p> <ul style="list-style-type: none"> - Reservrutiner och reservplaner för verksamheten, t. ex. alternativa administrativa rutiner och flytt till andra (förberedda) lokaler vid brand. - Plan för alternativ drift av enskilda IT-system, t. ex. plan för hur ett enskilt IT-systemet byggs upp igen med hjälp av reservdelar vars leveranstider kan garanteras. <p>Det är viktigt att dessa bägge typer av kontinuitetsplaner samspelar i de fall de är beroende av varandra.</p> <p style="text-align: right;">Ja Nej</p> <p>Kontinuitetsplaner finns för verksamheten <input type="checkbox"/> <input type="checkbox"/></p> <p>Dessa planer har testats så långt det är möjligt <input type="checkbox"/> <input type="checkbox"/></p> <p>Kontinuitetsplaner finns för de verksamhets-kritiska IT-systemen <input type="checkbox"/> <input type="checkbox"/></p> <p>Dessa planer har testats <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>
<p>Återstartsplaner</p> <p>Det ska finnas en dokumenterad, kommunicerad och testad rutin för återstart av IT-systemen (normal återstart).</p> <p>Det ska även finnas en återstartsplan dvs. en plan för att återstarta IT-system och dess kommunikation efter olika typer av felsituationer.</p> <p>Observera att det finns beroenden mellan vissa system som gör att systemen kanske måste återstartas i en viss turordning.</p> <p style="text-align: right;">Ja Nej</p> <p>Rutiner för normal återstart finns för alla IT-system <input type="checkbox"/> <input type="checkbox"/></p> <p>Det finns återstartsplaner som tar hänsyn till olika felsituationer hos de viktigaste IT-systemen <input type="checkbox"/> <input type="checkbox"/></p>	<p>Noteringar</p>

EFTERLEVNAD AV LAGAR

Skydd av personuppgifter	Noteringar
<p>Enligt personuppgiftslagen (PUL) är huvudregeln att bearbetning av personuppgifter i IT-system endast får ske om berörda personer givit sitt samtycke. Detta innebär att det måste finnas en förteckning över vilka IT-system som har sådan bearbetning och av förteckningen ska det också framgå att berörda personer givit sitt samtycke till bearbetningen eller om så inte är fallet vilken är den laga grunden för bearbetningen.</p>	
<p style="text-align: right;">Ja Nej</p>	
<p>Det finns ett register över vilka IT-system som bearbetar personuppgifter med angivande av syftet med bearbetningen</p>	<p style="text-align: right;"><input type="checkbox"/> <input type="checkbox"/></p>
<p>De personer vars personuppgifter bearbetas av IT-system har givit sitt samtycke till att så sker</p>	<p style="text-align: right;"><input type="checkbox"/> <input type="checkbox"/></p>
<p>Annan laga grund för bearbetning med angivande av relevant bestämmelse i PUL</p>	<p style="text-align: right;"><input type="checkbox"/> <input type="checkbox"/></p>

LITEN ORDLISTA

Användardokumentation	Handböcker och/eller lathundar som beskriver hur man använder systemet.
Användare	Den person som tilldelats behörighet till IT-systemet och dess information.
Applikation	Ett dataprogram eller någon annan tillämpning med viss bestämd funktionalitet, t. ex. ett Excel-ark.
Incident	Händelse som potentiellt kan få eller kunnat få allvarliga konsekvenser för verksamheten. Även händelser som skadat verksamheten brukar kallas incident.
Informationstillgångar	En organisations informationsrelaterade tillgångar. Exempel på sådana tillgångar är: <ul style="list-style-type: none"> • Kunddatabas, metodik, dokument • Egenutvecklad programvara • Tjänster såsom nätförbindelser och abonnemang
Skyddsvärda tillgångar	I detta sammanhang avses: <ul style="list-style-type: none"> • maskinvaror (datorer, skrivare, lokala nätverk och annan utrustning) • programvaror • informationstillgångar (se dito)
SLA	En överenskommelse som träffats mellan systemägare och systemförvaltare.
System	Någon generell heltäckande definition på begreppet "system" finns ej, men gemensamt för alla system är att de är resultat av människors tankemöda. Följande gäller ofta för ett system: <ul style="list-style-type: none"> • Det fyller ett behov (anledningen till att systemet skapades) • Det ger ett resultat (abstrakt eller konkret som man har viss användning för) • Det skapar en effekt i verksamheten (som ibland benämns nytta). Effekten ska ställas mot behovet, dvs. om systemet motsvarar förväntningarna, matchar nyttan det ursprungliga behovet. Ett IT-system beskrivs ofta i termer av: <ul style="list-style-type: none"> • Funktionalitet • Kapacitet • Säkerhet (m.a.p. sekretess, riktighet och tillgänglighet) • Struktur • Avgränsningar mot omvärlden • Funktionsberoenden gentemot omvärlden • Utbyte av information med omvärlden
Systemförvaltare	Den person som ansvarar för den dagliga driften av systemet.
Systemägare	Den person som ansvarar för systemets budget och att systemet uppfyller verksamhetens krav på funktionalitet, kapacitet och säkerhet (uttryckt i sekretess, riktighet och tillgänglighet).

Bilaga 10

AVVIKELSE- OCH HÄNDELSEHANTERING

Den här blanketten är framtagen för att underlätta för det drabbade företaget att strukturera det misstänkta brottet som man utsatts för samt underlätta den fortsatta hanteringen. Det finns ett flertal andra sätt att rapportera avvikelser och händelser exempelvis via webbaserade system. Det viktigaste är att företaget hittar ett eget sätt att hantera avvikelser och händelser.

Rapporten ligger sedan till grund för bedömning, analys samt eventuella föreslagna åtgärder med anledning av det inträffade.

Företag:

Händelsedatum: Tidpunkt:

Tjänsteställe, handläggarens namn, fax och telefon:

Belägenhet:

Större tätort Övrig tätort, förort Landsbygd

Anläggningens (motsvarande) adress/geografiska belägenhet:

INCIDENT/HÄNDELSE

Intrång

- Intrångsförsök
 Inbrott
 Obehörig närvaro
 Nyckel/nyckelkort anv.

Skadegörelse

- Åverkan
 Vandalisering
 Sabotage
 Brand

Hot

- Mot person
 Mot anläggning

Manipulation

- Bortkoppling
 Obehör. nyttj./omkoppling
 Förändring/förstöring
 Avlyssning/avtappning
 Forcering/simulering av:
 IT-system
 IT-system drift
 ADB-system adm.

Tillgrepp

- Stöld
 Rån/överfall

Sekretess

- Obehörig åtkomst
 Otillåtet röjande
 Dataintrång

OBJEKT/BYGGNADER**Produktionsanlägggn.**

- Vattenkraft
 Kärnkraft
 Olja
 Biobränsle
 Gas
 Kol
 Värme

Ledning

- 400 kV
 220 kV
 70-130 kV
 20-40 kV
 6-10 kV
 Lågspänning
 Gas
 Fjärrvärme

Nätstation

- 220-400 kV
 130 kV
 6-40 kV
 Lågspänning
 Transformerering
 Kompensering
 Manöverhus
 MR-station

Driftövervakningsanlägggn.

- Driftcentral, central
 Driftcentral, regional
 Driftcentral, lokal
 Kommunikationsanlägggn.
 Radiomast

Adm. byggnad

- Kontor
 Datalokal
 Kurs-/samlingslokal

Övrigt

- Verkstad
 Förråd
 Garage
 Upplag
 Inhägnad

Byggarbetsplats

- Produktionsanl.
 Transformatorstn.
 Adm. byggnad

Tillfällig arbetsplats/fordon

- Fältarbetsplats
 Personalvagn
 Bil

FÖRLUST/SKADA

- Pengar
 Värdehandlingar
 Ritningar
 ADB-lagrad info.
 Programvara
 Instrument

- Beh. kort/-kod
 Ftg-hemlig info
 Elapparater
 Radioutrustn.
 Verktyg
 Kabel/metaller

- Datorutrustn.
 TV/video
 Kontorsutrustn.
 Nycklar/nyckelkort
 Byggnader
 Staket

- Arbetsmaskin
 Fordon
 Drivmedel/fordonsutrustn.

Polisanmälan:

- Ja Polisrapport bifogas Nej

Fotografier bifogas:

- Ja Nej

Övriga upplysningar (exempelvis händelseförlopp):

UPPSKATTADE KOSTNADER

Värdet av förlorad egendom:

Arbetskostnader:

Uteblivna intäkter:

Övrigt:

Totalkostnad:

Säkerhetschefs kompletteringar (sekretess m. m.):

Datum: Underskrift:

Företag/avd:



**ENERGIGAS
SVERIGE**

Energigas Sverige

Box 49134, 100 29 Stockholm

Tel 08-692 18 40 | Fax 08-654 46 15

E-post info@energigas.se

www.energigas.se



**SVENSK
energi**

Svensk Energi

101 53 Stockholm

Tel 08-677 25 00 | Fax 08-677 25 06

E-post info@svenskenergi.se

www.svenskenergi.se



Svensk Fjärrvärme

Svensk Fjärrvärme AB

101 53 Stockholm

Tel 08-677 25 50 | Fax 08-677 25 55

E-post kontakt@svenskfjarrvarme.se

www.svenskfjarrvarme.se



**SVENSKA
KRAFTNÄT**

Svenska Kraftnät

Box 1200, 172 24 Sundbyberg

Tel 08-475 80 00 | Fax 08-475 89 50

E-post [registrator@svk](mailto:registrator@svk.se)

www.svk.se