

Företagssäkerhet

Företagssäkerhet handlar om säkerhet i företagets hela verksamhet. Med hjälp av företagssäkerhet kan man skydda värderingar som är viktiga för företaget, såsom personer, information, anseende, egendom och miljö.

En central uppgift för företagssäkerhet är att främja och säkerställa företagets konkurrenskraft och förbättra produktiviteten. Säkerhetsledning utgör en del av normal företagsledning. Målet är inte en separat säkerhetsfunktion utan säkerställande av företagsverksamhetens kontinuitet, säkerhet och kravenlighet i alla situationer som en naturlig del av företagets riskhantering.

Företagssäkerhetsmodellen för näringslivet är avsedd för företag av olika storlek. Modellen kan dock tillämpas på olika organisationer såsom myndigheter och andra sammanslutningar.

1 Identifiera hot, bedöm risker och var beredd

I en grundläggande ordbok i definieras hot som en ogynnsam, skrämmande eller skadlig omständighet som eventuellt kan realiseras. Enligt den internationellt använda riskhanteringsstandarden ISO 31000 är risk en osäkerhetsfaktors inverkan på målet.

Det rekommenderas att företag gör en övergripande kartläggning av säkerhetshot och de risker som de eventuellt medför för företaget. Identifiering av hot samt bedömning och hantering av risker är en central förutsättning för definitionen och dimensioneringen av målen och metoderna för företagssäkerhet. Säkerhets- och sårbarhetsanalyser utgör en del av identifiering av hot, bedömning av deras betydelse och beredskap för dem. Det är motiverat att engagera företagets centrala intressenter och samarbetspartner i identifieringen, bedömningen och hanteringen av risker. Det gäller att fortlöpande hålla ett öga på företagets riskmiljö, eftersom säkerhet är hantering av förändringar. Säkerhetsverksamheten och riskhanteringen syftar inte endast till att eliminera eller minska risker utan även att möjliggöra risktagande för företaget – affärsverksamhet baserar sig på risktagande, men det är viktigt att systematiskt identifiera, bedöma och hantera risker. Om en oidentifierad risk realiseras kan konsekvenserna bli ödesdiga.

2 Öka medvetenheten, utbilda och uppmuntra

Man kan hitta utvecklingsobjekt för säkerhetsverksamheten till exempel genom att granska statistik över avvikelser, olycksfall och skador, och genom att lära av deras grundorsaker. Det är motiverat att satsa på utarbetandet av högklassiga säkerhetsanvisningar och implementeringen av dem i praktiken.

Det är mycket viktigt att utbilda personal, öka säkerhetsmedvetenheten och skapa en god säkerhetskultur. Företag behöver också lednings- och kommunikationssystem för säkerhet med vars hjälp man kan trygga företagsverksamhetens kontinuitet i alla situationer. Det är motiverat att ge personal och intressenter respons i säkerhetsfrågor och uppmuntra dem att beakta säkerheten i all verksamhet.

Med tanke på utvecklingen av säkerheten är det viktigt att analysera förändringar i både den interna och externa operativa miljön. I analysen av den senare får man hjälp av myndigheters lägesöversikter och rapporter.

3 Sträva efter kvalitet, använd standarder och satsa på samarbete

Säkerhet är en del av företagets kvalitetssystem och ger även kunder mervärde. Därför är det motiverat att företaget förbinder sig till att fortlöpande utveckla säkerhetsverksamheten. Säkerhet är inte ett permanent tillstånd utan en fortlöpande process. Säkerhetsverksamhetens standarder, kvalitet och indikatorer ger företaget och dess samarbetspartner en tydlig bild av verksamhetens nivå utan en detaljerad genomgång av företagsspecifika frågor.

När det gäller säkerhetsfrågor är det motiverat att nätverka med andra aktörer. Genom intressentsamarbete med andra företag, myndigheter och säkerhetsexperter strävar man efter att få information om säkerhetshot och agera effektivt vid eventuella störningar, till exempel i bekämpningen av olycksfall, skador och brott. Nätverk har ofta också värdefull kunskap om vilka säkerhetsåtgärder som fungerar.

4 Vad omfattar företagssäkerhet?

EK har utvecklat en företagssäkerhetsmodell, vars olika områden bildar en grund för analysen av företagets säkerhetsfält. Dessa områden kan delvis överlappa varandra. Det är viktigt att notera att företagets bransch och affärsverksamhet alltid påverkar de olika områdenas betydelse. Alla områden är inte nödvändigtvis lika viktiga för alla företag. Det som är väsentligt är att välja de viktigaste områdena och åtgärderna med tanke på den egna organisationen. Modellen beaktar också vikten av fortlöpande utveckling av verksamheten. Modellen är direkt tillämplig på en internationell miljö. Det är dock alltid viktigt att analysera och beakta lokala förhållanden, lagstiftning och risker.



Bild 1: Företagssäkerhetsmodell

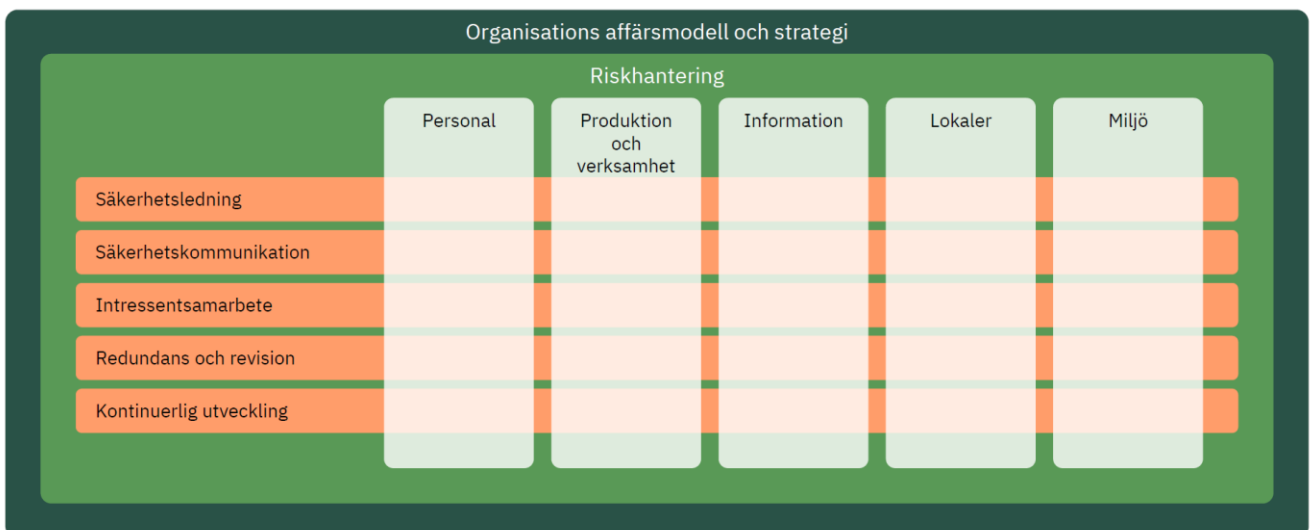


Bild 2: Företagssäkerhetsmodell som en matris

Personalsäkerhet

Personalsäkerhet är en viktig del av organisationens säkerhet. Syftet med personalsäkerhet är att garantera människors säkerhet och funktionsförmåga genom att skydda dem mot brott och olyckor. Dessutom säkerställs kritiska personresurser för organisationens verksamhet.

Personalsäkerhet består av bland annat följande områden:

1) Skyddande av medarbetare, kunder och nyckelpersoner mot brott och olyckor	
• Kunders och besökares säkerhet • Säkerhet på resor och i utlandsarbete	– Resehandlingar – Säkerhetsanvisningar – Kommunikationsförbindelser och -utrustning – Larm- och jourtjänster – Evakueringsanvisningar – Försäkringar – Riskklassificering av länder och regioner – Relevanta utbildningar
• Nyckelpersoners säkerhet	– Begränsning av kontaktuppgifters tillgänglighet (t.ex. spärrmarkering, förbud mot utlämnande av adressuppgifter) – Säkerhetsteknik – Personskydd i särskilda fall – Hot- och riskanalys samt planering och dimensionering av åtgärder därefter
• Hemmets och familjens säkerhet	– I arbete i hemlandet och utlandet

**2) Säkerställande av personalresurser som är kritiska för verksamheten**

- Ersättare och vikarier
- Tillgänglighetsarrangemang
- Personalberedskap för kriser om möjligt

– Säkerställande av larm- och kommunikationsrutiner

3) Skyddande av verksamheten mot brottslig infiltrering etc.

- Omsorgsfull och högklassig rekrytering
- Säkerhetsutredningar
- Sekretessavtal och -förbindelser
- Drogtestning
- Testköp (inom handel)

Fastighets- och lokalsäkerhet

Organisationens verksamhetsställen och lokaler bör skyddas kostnadseffektivt baserat på riskbedömningar. Målet är att skapa en störningsfri och säker arbets- och servicemiljö samt förhindra att information eller material som är värdefulla för organisationen blir stulna.

Fastighets- och lokalsäkerhet består av bland annat följande områden:

1) Säkerhetsklassificering av lokaler och skyddande av dem enligt klassificeringen

- Skapande av säkerhetszoner enligt skyddade objekt och funktioner (jämför med cyber- och informationssäkerhet)
- Utnyttjande av principen om perimeterskydd
- Beakta också objektets miljö och miljörelaterade risker som påverkar den egna säkerheten

2) Strukturell säkerhet

- Planering av miljöns säkerhet (läge, parkering, lastning och lossning)
- Användning av stängsel, portar, körhinder och belysning
- Lås och nyckelhantering samt administration av åtkomsträttigheter
- Inbrottsskydd och säkerhetskonstruktioner
- Värdeförvaringsenheter (kassaskåp, säkerhets- och brandskyddsskåp, valv)
- Fastighetsteknik
- Befolkningsskydd
- Tillgänglighet

3) Säkerhetsövervakning

- Teknisk säkerhetsövervakning (passerkontroll, brottsdetektorer/inbrottslarm och kameraövervakning)
- Eskort och övervakning av personal, besökare och fordon på områden och i lokaler
- Bevakning och monitorering
- Mötes- och förhandlingslokalers säkerhet

4) Avtalshantering

- Outsourcing och köpta tjänster (bl.a. service, städning samt fastighets- och säkerhetstjänster)

- Underhålls- och serviceavtal, inspektioner
- Bygg- och renoveringsprojekt
- Ansvarsfrågor och försäkring

Räddningssäkerhet

Med räddningssäkerhet avses förebyggande av bränder och andra olyckor samt en snabb och relevant respons vid olyckor.

Det är viktigt att hantera olycksfallsrisker med hjälp av förutseende, eliminering, minimering och försäkring. Dessutom gäller det att beakta planerings- och beredskapsskyldigheterna samt räddningslagstiftningen och myndigheternas anvisningar och föreskrifter. Det är viktigt att utarbeta säkerhetsanvisningar och ordna regelbunden utbildning för personalen med tanke på olycksfall. Dessutom gäller det att utveckla allmänna medborgarfärdigheter såsom principerna om förstahjälp och primärläckning.

Räddningssäkerhet består av bland annat följande områden:

1) Räddningsplan som styrande dokument	
• Förutseende av risker • Arbetsplatsspecifika arrangemang • Utomhusområden (arbete eller evenemang) • Beredskap för storolyckor • Åtgärder för att bekämpa hot	– Anvisningar – Strukturella åtgärder – Ansvariga personer – Regelbunden utbildning – Bevakning och passerkontroll – Förstahjälp – Räddnings-, reparations-, röjnings- och underhållsåtgärder
2) Brandsäkerhet	
– Byggnaders brandsäkerhet – Service och regelbunden inspektion av räddnings- och släckningsutrustning – Säkerhet i heta arbeten	– Klassificering och sektionering – Automatiska branddetektionssystem – Beaktande av bärande konstruktioner – Räddnings- och släckningsarrangemang – Utrustning för primärläckning – Säkerhets- och informationsbelysning – Säkerhetsinstruktioner – Automatisk släckningsutrustning – Rökventilation – Förebyggande av mordbränder
3) Försäkring	

- | | |
|---|--|
| <ul style="list-style-type: none">• Egendoms- och avbrottsförsäkring• Försäkringsbolagens skyddsanvisningar och -villkor | |
|---|--|

Syftet med produktionens och verksamhetens säkerhet är att garantera säkra produkter och tjänster.

Produktionens och verksamhetens säkerhet består av bland annat följande områden:

1) Produktansvar och -säkerhet
• Aktsamhets- och anmälningsskyldighet • Tillsynsmyndigheter • Riskbedömning • Märkningar (t.ex. CE)
2) Servicesäkerhet
3) Betalningssäkerhet
4) Förvaring av värdefull egendom
5) Logistisk säkerhet (transport och lagring)
• Hantering av leveranssätt • Fastställande av ansvarsområden
6) Nätverk
• Underleverantörer och tjänsteleverantörer • Avtalshantering
7) Försäkring
• Ansvarsförsäkring • Egendomsförsäkring • Produktförsäkring • Avbrottsförsäkring

- Projektförsäkring
- Transportförsäkring

Syftet med miljösäkerhetsverksamheten är att beakta ekologisk hållbarhet samt bemöta och förutse kundernas och samhällets miljörelaterade förväntningar. Detta innebär miljöåtaganden, fortlöpande utveckling av processer och bästa praxis, ökning av personalens medvetenhet, iakttagande av lagstiftning och standarder samt öppen kommunikation.

Miljösäkerhet består av bland annat följande områden:

1) Principer för hållbar utveckling
2) Energieffektivitet
3) Omsorgsfull bedömning av miljökonsekvenser
4) Anmälnings- och tillståndsförfaranden
5) Hantering och lagring av farliga ämnen
6) Hanteringssystem och handlingsprogram för miljöskydd
7) Klimatskydd och utsläppshandel
8) Skydd av vattendrag och mark
9) Bullerbekämpning och landskapsskydd
10) Kemikalieövervakning
11) Avfallshantering

Informations- och cybersäkerhet

Informations- och cybersäkerhet är en viktig del av organisationens säkerhet. Med informations- och cybersäkerhet avses i allmänhet bland annat informationens konfidentialitet och integritet, informationssystemens och tjänsternas kontinuitet, fysiskt skydd, leveranskedjor och externa krav med beaktande av människor, processer och teknik.

Eftersom den tekniska utvecklingen är snabb, krävs det fortlöpande analys av metoder och utveckling av åtgärder. Det är omöjligt att uppnå absolut säkerhet, och därför gäller det att satsa på verksamhetens kontinuitet inom informations- och cybersäkerhet.

Organisationens cyber- och informationssäkerhet består av bland annat följande områden:

1) Bedömning av informationens betydelse	
• Administration av kritisk information och annan egendom samt identifiering av funktioner som är viktiga med tanke på säkerheten • Informationens användbarhet, integritet och konfidentialitet	– Certifikat och verifierbarhet
2) Klassificering och hantering av information	
• Klassificeringsmetoder • Klassificeringsanvisningar som omfattar informationens hela livscykel	– Klassificeringssystem – Beakta både digitala och fysiska informationsbehandlingsmiljöer
3) Administrativ informationssäkerhet	
• Administration av användar- och åtkomsträttigheter • Säkerhetsutredningar • Säkerhetsavtal • Sekretessavtal och -förbindelser	
4) Data- och integritetsskydd	

• Behandling av personuppgifter • Integritetsskydd i arbetslivet • Kommunikationsskydd	
5) Teknisk informationssäkerhet	
• Kommunikationsnätverkets strukturella säkerhet • Observation och förhindrande av skadlig datakommunikation • Spårbara funktioner och monitorering av dem • Uppdaterad programvara • Säker konfiguration av utrustning och programvara • Nätverkssegmentering • Identitets- och åtkomsthantering • Utveckling av användarnas kompetens	– Tjänster (e-post etc.) – Telefoner, mobila enheter – Personalens kompetens
6) Säkerställande av systemens och processernas kontinuitet	
• Utveckling av observationsförmågan • Utveckling av resiliensen och återhämtningsförmågan • Informationsbehandlingsmiljöns fysiska säkerhet • Tekniskt och strukturellt skydd av kritisk fysisk utrustning, till exempel korskopplingsskåp • Säkerhetskopiering • Återhämtningsplanering • Krishantering • Hantering av den övriga verksamhetens kontinuitet	– Fortlöpande observation, logguppföljning – Störningsberedskap

Hantering av missbruk och avvikelser

Med hjälp av hantering av missbruk och avvikelser förebygger och utreder organisationen missbruk, brott och andra avvikelser som påverkar verksamheten. Det är fråga om att skydda organisationens verksamhet, personal och egendom mot interna och externa hot.

Hantering av missbruk och avvikelser består bland annat av följande områden:

1) Skadliga händelser riktade mot verksamheten, personalen och egendomen	
• Observation, analys och förebyggande av skadliga händelser • Lösningssmodeller och återhämtning • Rapportering och lärande	– Externa händelser – Interna händelser
2) Metoder för hantering av missbruk	
• Förebyggande åtgärder • Avslöjande • Interna revisioner och utredningar • Samarbete med myndigheter • Agerande vid brott	– Planering, strategi och tekniska lösningar – Preliminära utredningar – Brott som leder till förundersökning – Målsägarbrott – Brott under allmänt åtal
3) Försäkring	
• Brottsrisker	

Beredskap och krishantering

Med hjälp av beredskap och krishantering strävar organisationen efter att identifiera och förebygga oväntade situationer och att skydda sig mot dem så effektivt som möjligt. Störningar kommer ofta som en överraskning och kräver snabba beslut. Därför är det viktigt att förhandsplanera och ordna övningar.

Organisationen bör bevara sin handlingsförmåga och sträva efter att återhämta sig så snabbt som möjligt. Det är fråga om säkerställande av verksamhetens kontinuitet i alla situationer. Krishantering står således i nära växelverkan med kontinuitetsplanering (*business continuity management*).

Beredskapsplanering, som avses i beredskapslagstiftningen, baserar sig på försvarsekonomisk planering och säkerställande av försörjningsberedskapen i undantagsförhållanden. Beredskapsplanering gäller i synnerhet företag som är kritiska med tanke på försörjningsberedskapen och vars tjänsters kontinuitet det är viktigt för hela samhället att säkerställa i undantagsförhållanden. Alla organisationer bör dock säkerställa sin verksamhet med tanke på kriser.

1) Kontinuitetsplanering	
• Bedömning av affärsrisker och planering av alternativa tillvägagångssätt • Avbrott eller stopp i produktionen • Planering och utveckling av resiliensen	– Lönsamhet – Avtal
2) Krishantering	
• Förebyggande och bedömning • Agerande i kriser • Återhämtningsplaner • Lärande	– Beredskap – Akuta kriser – Kriser som utvecklas – Snabb och adekvat respons – Kommunikation
3) Beredskapsplanering (beredskap för undantagsförhållanden)	

- Identifiering av skyldigheter
- Produktions- och verksamhetsplanering

- Personberedskap (VAP)
- Energiförsörjning
- Materiallagring
- Råvaror, maskiner och utrustning
- Fördonsberedskap vid behov
- Reparation och underhåll, reservdelar
- Underleveranser och tjänster

Målet för arbetssäkerhetsverksamheten är säkra arbetsförhållanden, medarbetarnas välbefinnande och därigenom en god och ansvarsfull företagsimage.

Verksamheten styrs av arbetarskyddslagstiftningen, som fastställer rutinerna och miniminivån för arbetarskyddet. Arbetssäkerhet skapas med hjälp av ett målinriktat åtgärdsprogram som innehåller konkreta åtgärder för att förebygga hälsoolägenheter relaterade till arbetet.

1) Säkra arbetsförhållanden och medarbetarnas välbefinnande – förebyggande av risker och en god företagsimage	
• Arbetssäkerhetsledning och -samarbete på arbetsplatsen • Arbetarskyddsfullmäktige • Arbetssäkerhet på arbetsplatsen • Säkerhet relaterad till maskiner, utrustning och arbetsredskap • Intern trafik på arbetsplatsen • Fysikaliska faktorer • Psykosociala belastningsfaktorer • Hantering av farliga ämnen • Kemikalieexponering • Personlig skyddsutrustning • Bemötande av våld och hot om våld • Arbetshälsa • Arbetssäkerhet på en arbetsplats där flera företag är verksamma	– Arbetsgivarens arbetarskyddsuppgifter – Arbetstagarnas arbetarskyddsuppgifter – Arbetarskyddssamarbete – Företagshälsovård – Arbetsgemenskapens funktionsförmåga – Verksamhet som upprätthåller arbetsförmågan
2) Arbetarskyddsorganisation	
• Arbetarskyddskommission, arbetarskyddschef, arbetarskyddsfullmäktige, arbetarskyddsombud	
3) Verksamhetsprogram	

• Mål	– Fortlöpande förbättring av arbetshälso- och arbetssäkerhetsnivån som en fråga som rör hela arbetsgemenskapen – Utveckling av rutiner, förhållanden och verktyg – Involverande av samarbetspartner – Utveckling av den arbetsplatsspecifika verksamheten – Ledning av arbetsförmågan som en del av den strategiska ledningen – Främjande av arbetsförmågan och -miljön med hjälp av proaktiv företagshälsovård – Ökning av säkerhetsmedvetenheten
• Utbildning	– Introduktion, arbetssäkerhetskort, specialuppgifter, utlandsverksamhet
• Indikatorer	– Kvantitativa och kvalitativa indikatorer
• Statistik	– Olycksfallsstatistik – Rapporter om incidenter (tillbud) – Statistik över sjukfrånvaro

Standard/standardserie		
Standardserie för kvalitetshantering	ISO 9000	
Riskhantering	ISO 31000 ISO 31010	
System för hantering av leverantörskedjors säkerhet	ISO 28000	
Säkerhet och resiliens Standardserie för miljöledning	ISO 22301 ISO 14000	
Standardserie för informationssäkerhet	ISO/IEC 27000	
Standardserie för egendomsförvaltning	ISO 55000	
Ledning av företagshälsovård och arbetssäkerhet	ISO 45001	
Samhällsansvar	ISO 26000	
Energihantering	ISO 50001	