Næringslivets sikkerhetsråd

Sikkerhet ved etablering i utlandet

En veileder i etablering i utlandet for små og mellomstore virksomheter

Forord

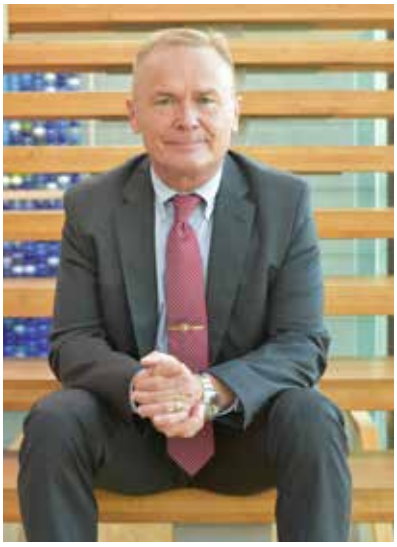
Vi kommer fra et fredelig land med en kultur som baserer seg på tillit. Tillit er limet i samfunnet vårt, og tillit gjør oss effektive. Vi stoler stort sett på hverandre, og vi får jobben gjort. Tilliten vi har til hverandre gjør blant annet Norge til et av verdens beste land å bo i. Men tillit ikke er en universell størrelse, og kan ikke defineres i henhold til en internasjonal standard.

Verden er et mangfold av kulturer, og hver kultur har sitt syn på verdier, mennesker og tillit. Det må vi ta med i våre vurderinger når vi skal virke utenlands. Tillit basert på uriktige premisser og manglende kunnskap, blir fort til naivitet. Og naivitet bidrar sjelden verken til personlig sikkerhet eller gode forretninger.

Vi reiser mye, både i jobb og fritid, og stadig flere store og små bedrifter ønsker å etablere seg utenlands for å styrke sine posisjoner. Dette er en utvikling som er ønsket, både fra næringsliv og myndigheter. Dersom forberedelsene er tilfeldige, og beslutningene er basert på mangelfulle eller fravær av analyser, kan en etablering utenlands være både risikofull og vanskelig.

I denne veilederen tar vi opp noen relevante problemstillinger du og din bedrift bør vurdere dersom dere tenker på å etablere dere utenlands.

God lesning og lykke til med den internasjonale satsingen.



Odin Johannessen
Direktør i Næringslivets Sikkerhetsråd

Innhold

1. Bakgrunn og formål

Et økende antall norske virksomheter etablerer seg i utlandet. Etablering i utlandet med fører eksponering til nye og fremmede miljøer. Denne eksponeringen kan medføre økt risiko, og spesielt sikkerhetsrisiko. Denne risikoen må forstås og håndteres.

Ofte starter utfordringene lenge før virksomheten tar beslutningen om å etablere seg i utlandet, ved at ansatte reiser til og fra det utvalgte landet for å kartlegge og tilrettelegge for etableringen. Allerede da møter virksomhetens ansatte en annen kultur, språk, måte å gjøre forretninger på og det som dette infoheftet fokuserer på, nemlig en annen sikkerhetssituasjon enn virksomheten er kjent med fra Norge.

Det er derfor viktig at virksomheten forbereder seg godt. Gjennom grundig planlegging og analyser av det landskapet virksomheten skal etablere seg i bør nødvendige tiltak identifiseres og implementeres. På den måten kan virksomheten unngå å havne i uønskede situasjoner som i ytterste konsekvens kan sette hele utenlandsetableringen på spill.

1.1 Informasjonsheftets formål

Informasjonsheftets formål er å gi små og mellomstore virksomheter noen råd om hva de bør tenke gjennom når det gjelder sikkerhet ved etablering i utlandet. Informasjonsheftet retter seg i hovedsak mot virksomhetens funksjoner som er involvert i planlegging av utenlandsetableringen. Imidlertid kan informasjon med fordel distribueres bredt blant alle ansatte for å skape bedre forståelse for utfordringene og bidra til kulturbygging. Erfaringene i dette informasjonsheftet er basert på god praksis fra større virksomheter i Norge med erfaring fra etablering i utlandet.

Informasjonsheftet er ikke utfyllende. Hensikten er å gi et grunnlag for forståelsen av kompleksiteten av utfordringer og en refleksjon rundt noen av de vanligste utfordringene norske virksomheter kan møte i denne prosessen.

Selv om informasjonsheftet er utarbeidet for virksomheter som vil etablere seg i utlandet, så har det også gyldighet for virksomheters aktiviteter og operasjoner i Norge.

1.2 Avgrensning

I Norge favner begrepet sikkerhet ofte om både det som på engelsk kalles *security* og *safety*. Det kan lede til misforståelser og sammenblanding av begreper. I dette informasjonsheftet vil derfor ikke Safety (eller farer på norsk) bli diskutert. Faktorer knyttet til for eksempel helse og sykdom, trafikksikkerhet, klima og naturkatastrofer osv. vil ikke bli diskutert. Imidlertid bør disse faktorene inkorporeres i beredskapsplanverket til virksomheten i forbindelse med utenlandsetableringen. Informasjonsheftets fokus vil være på trusselaktører (mennesker) som har intensjon og/eller kapasitet til å utføre en villet ondsinnet handling for å skade, tilrøve seg en fordel eller på annen måte ødelegge for virksomheters aktivitet.

Begrepsavklaring

Safety has to do with the protection against hazards, and companies generally control means to manage them prudently. Security, on the other hand, is about protection against threats. The origin of those threats and the likelihood of their arising in specific circumstances are usually beyond the control of companies. The most that can normally be done is to mitigate through reducing vulnerability and building resilience so that potential attackers can be discouraged, and incidents can be rapidly responded to and periods of disruption minimized. This is as true of cyber security as of terrorist attacks. *Kilde: Statoil ASA. The In Amenas Attack.*

2. Hovedområder

Det er tre hovedområder av sikkerhet: fysisk-, informasjons- og personellsikkerhet.

Fysisk sikkerhet handler om de tiltak virksomheten iverksetter for å beskytte seg mot uautorisert adgang til virksomhetens fasiliteter i den hensikt å beskytte seg mot tyveri, sabotasje og skader.

Eksempler på trusler mot fysisk sikkerhet kan være industrispionasje eller sabotasje som kan medføre at hemmeligheter blir stjålet, eller at produksjonen blir forsinket eller stanset. Terrorvirksomhet, væpnede angrep, væpnet konflikt/krig eller politisk motivert vold kan ramme direkte eller indirekte og kan medføre betydelig risiko for virksomhetens ansatte. Kidnapping og utpressing er velkjente handlemåter i enkelte deler av verden og kan skape betydelige utfordringer virksomheten (se også NSRs veileder om tigerkidnapping av 2017).

Aktivister som ønsker å fremføre sitt budskap kan benytte virksomheten for å få oppmerksomhet. Pirater kan for eksempel overta kommando over fartøyer og kreve løsepenger for frigivelse av last og fartøy.

Fysisk sikkerhet handler blant annet om adgangskontroll, kameraer, gjerder, dører, vakter, reisesikkerhet for ansatte, sikring av en bedrifts topplede delse og sikring av informasjon (eks: servere).

Informasjonssikkerhet handler om de tiltak virksomheten iverksetter for å beskytte konfidensialitet, integritet og tilgjengelighet av virksomhetens systemer, nettverk og data. Informasjonssikkerhet inkluderer også kontroll på fysiske dokumenter, hva man snakker om hvor, og om det for eksempel er enkelt innsyn i virksomhetens lokaler. Her er det viktig å huske på at informasjon må kunne distribueres internt og eksternt, men det er viktig å skille mellom hvem som kan få tilgang til hvilken informasjon/hemmeligheter.

Eksempler på trusler mot informasjonssikkerheten kan være cyberangrep mot virksomheten som kan skade tilgjengelighet og integritet på data, eller DDoS angrep. Uautorisert tilgang til nettverk er en annen trussel mot informasjonssikkerheten. Malware som virus, trojanere, phishing eller annen ondsinnet programvare sendes til ansatte i virksomheten i den hensikt å skade systemer, nettverk eller data. Social engineering kan forekomme via e-post eller sosiale medier hvor utenforstående forsøker å få tilgang til ansatte i virksomheten for å manipulere dem til å for eksempel utlevere informasjon, bevisst eller ubevisst. Sensitiv og gradert informasjon kan stjeles eller deles av ansatte eller kontraktører med legitim tilgang til informasjon i virksomheten.

Personellsikkerhet handler om de tiltak virksomheten iverksetter for å beskytte seg mot de som allerede har legitim tilgang til virksomheten og dets system, nettverk og data og som kan tenkes å utnytte dette til egen vinning, eller blir utnyttet av andre til å begå en kriminell handling mot virksomheten. Innsidere er ofte brukt som begrep på disse personene.

Eksempler på trusler kan være ansatte som blir sagt opp eller er misfornøyde, ulovlige aktivister, konkurrenter, kriminelle, terrorister eller statlige aktører som blir ansatt for å få tilgang og påvirke på sin måte. Innsidere kan også være tvunget til å utlevere informasjon om virksomheten gjennom utpressing fra utsiden av virksomheten. Ansatte eller kontraktører med forfalskede vitnemål/kursbevis kan utgjøre en betydelig sikkerhetsrisiko for virksomheten. HR-avdelingen har et spesielt ansvar når det gjelder personellsikkerhet, og bør samarbeide tett med sikkerhetsavdelingen for å holde seg orientert om personellsikkerhetsutfordringer.

Se forøvrig veileder fra Næringslivets sikkerhetsråd av 2018: *Sikkerhet ved ansettelsesforhold*.

Fysisk sikkerhet. Virksomheten bør:

- vær observant på forhold til omgivelsene og rapporter avvik til nærmeste overordnede eller sikkerhetsleder (sørg for at rapport også ender opp i Norge)
- være nøye med at kun de som har legitim adgang til virksomhetens fasiliteter får komme inn
- sørge for at ansatte har kontroll på sine eiendeler
- rapportere mistenkelig aktivitet til nærmeste leder og sikkerhetsleder.

Informasjonssikkerhet. Virksomheten bør:

- bruke kryptering i flere lag, brannmurer og penetrasjondeteksjonssytemer
- beskytte brukernavn og passord samt elektroniske enheter
- forstå hvilken informasjon som må beskyttes spesielt
- rapportere mistenkelig aktivitet til nærmeste leder og sikkerhetsleder

Personellsikkerhet. Virksomheten bør:

- vurdere å gjennomføre bakgrunnssjekk av ansatte, spesielt de som er i nøkkelstillinger
- følge med på hvem du har rundt seg, og legge spesielt merke til endret livsførsel eller interesse for arbeidsfelt vedkommende ikke naturlig har ansvar for
- stimulere ansatte til å rapportere mistenkelig aktivitet til nærmeste leder og sikkerhetsleder.

3. Ansvar og plikter

Alle ansatte i virksomheten plikter å ha fokus på sikkerhet. Det er topplederen i virksomheten som er overordnet ansvarlig for sikkerheten. Imidlertid må alle ansatte påse at lover, regler, avtaler, instrukser og prosedyrer blir etterlevd.

Ingen virksomheter er sterkere enn det svakeste ledd. Det samme gjelder for virksomheter som etablerer seg i utlandet, som i tillegg kan få spesielle utfordringer knyttet til alt det ukjente og fremmedesammenlignet med det kjente i Norge. Det kan blant annet være et ukjent og komplisert kriminalitetsbilde, terrorvirksomhet, lovverk, korrupsjon og en annen sikkerhetskultur basert på et menneskesyn som ikke samsvarer med norske forhold. Derfor er det viktig at sikkerhetstenkningen gjennomsyrer organisasjonen, og at en sunn sikkerhetskultur vokser frem, hvor alle i virksomheten er seg sitt ansvar bevisst.

3.1 Myndighetskrav

Norske virksomheter som etablerer seg i utlandet forventes å forholde seg til norsk lov der hvor den er gjeldende, samt nasjonale lover i de landene de etablerer seg. Den viktigste norske loven å forholde seg til er arbeidsmiljøloven, som også dekker det såkalte «Duty of Care»- begrepet. Kort fortalt handler dette om hvordan arbeidsgiver har et ansvar for beskyttelse av egne ansatte når det gjelder helse, miljø og sikkerhet (HMS). Arbeidsmiljøloven og Internkontrollforskriften, tydeliggjør arbeidsgivers plikt til å kartlegge og vurdere risiko knyttet til arbeidsforhold i den hensikt å redusere risiko for virksomhetens ansatte.

Regelverket GDPR (General Data Protection Regulation) er like viktig å etterleve i utlandet som i Norge. Konsekvensen av å ikke etterleve GDPR, kan medføre en bot på opptil 4 % av årlig omsetning eller maksimalt 20 millioner euro. Alle relevante lover og regler må forstås og etterleves

3.2 Virksomhetens interne sikkerhetskrav

Virksomheter bør etablere et sett med interne sikkerhetskrav som alle i virksomheten skal følge. Etterlevelse av disse kravene er en forventing virksomhetens ledelse må stille til sine ansatte.

Sikkerhetsledelse må beskrives i de interne sikkhetskravene. Virksomhetens øverste leder er ansvarlig for sikkerheten. Imidlertid kan oppgaver delegeres i organisasjonen. En dedikert sikkerhetsleder, som også kan få oppfølgingsansvar for beredskap, bør pekes ut og denne bør kunne rapportere direkte til virksomhetens leder. Likeså bør det utpekes en sikkerhetsleder dersom virksomheten etablerer seg i utlandet. Det er viktig å påpeke at det ikke alltid er nødvendig å ha en full stilling for å bekle funksjonen som sikkerhetsleder, dette avhenger blant annet av omfanget av virksomhetens aktivitet og den generelle sikkerhetsrisikoen i landet.

Interne sikkerhetskrav må gjøres kjent for alle ansatte. Når virksomheten har etablert seg i utlandet, bør samme interne sikkerhetskrav i utgangspunktet gjelde for de lokalt ansatte som for virksomhetens norske ansatte. Det kan likevel differensieres mellom lokalt ansatte og utstasjonerte, og da særlig når det gjelder den tid den lokalt ansatte ikke er på jobb. På fritiden kan det imidlertid vurderes å innføre særskilte krav for lokalt ansatte med særlig eksponerte eller viktige stillinger dersom sikkerhetsvurderingen anser dette som nødvendig. Eksempler kan være profilerte ledere.

Standardisering og forenkling av sikkerhetskravene (og planer) er to nøkkelord som er viktige å tenke på når en etablerer seg i utlandet. En må i størst mulig grad gjennomføre aktiviteter på samme måte i Norge og i utlandet. Dette gjelder spesielt innenfor sikkerhet og beredskap, hvor det lett kan bli misforståelser om en

benytter forskjellige malverk for samme type aktivitet, for eksempel sikkerhetsplanen og beredskapsplanen. Husk også på at forenkling er nøkkelen til suksess. Lange kompliserte planer kan være nødvendig enkelte ganger, men ofte er det enkle det beste.

Opplæring i interne sikkerhetskrav er avgjørende for å lykkes, derfor bør det settes av tilstrekkelig med tid og opplæringen bør gjennomføres på et språk som alle ansatte forstår. Likeså er det viktig at opplæringen foregår på rett tidspunkt.

4. Risikovurdering

4.1 Sikkerhetsrisiko

Sikkerhetsrisiko består av tre faktorer: verdi, trussel og sårbarhet. En samlet vurdering av de tre faktorene gir *risiko*.

4.2 Verdi

Først og fremst må bedriftens verdier forstås. Verdier kan være mennesker, produkter, gjenstander, operasjoner, bygg og anlegg, og ikke minst informasjon. Vanligvis er virksomhetens viktigste verdier prioritert slik; 1) liv og helse, 2) naturmiljøet de jobber i, 3) de fysiske enhetene de er ansvarlige for og 4) omdømmet til virksomheten (på engelsk: PEAR). Imidlertid har virksomheter ofte noen «hemmeligheter» som de ønsker å beskytte ekstra godt. Det kan være patenterte løsninger, strategier og planer i forbindelse med oppkjøp, forskning og utvikling eller fysiske arkiver som bør beskyttes. Disse må analyseres og verdisettes, slik at man har et klart bilde av hva bortfall eller kompromittering av verdiene vil medføre av konsekvens for bedriften. Bedriften må etablere et klart bilde av hva som skal beskyttes fra en trusselaktør.

4.3 Trussel

En trusselaktør bestemmes primært ut fra dennes kapasitet og intensjon til å gjennomføre en ondsinnet, villet handling. Det kan være vanskelig å kartlegge en trusselaktørs intensjon og kapabilitet eksakt. Det vil alltid herske en viss usikkerhet omkring dette. Det må risikoanalysen ta høyde for.

For å forenkle risikovurderingen bør trusselaktører ordnes i grupper. Det enkleste er å gruppere dem i for eksempel a) kriminelle, b) terrorister, c) ulovlige aktivister, d) statlige aktører, d) lokalbefolkning og e) konkurrenter.

Hver av disse trusselaktørene kan gjennomføre sin ulovlige aktivitet på mange forskjellige måter. Fremgangsmåten kan også være lik for forskjellige trusselaktører, men det er viktig å forsøke å skille de forskjellige trusselaktørene fra hverandre. For eksempel kan alle trusselaktører ha både intensjon og kapasitet til å stjele fra virksomheten, men av forskjellig motiv. Det samme gjelder væpnet ran, sabotasje, hærverk etc. Dersom det er terror eller organiserte kriminelle grupperinger som er trusselen, bør disse beskrives med navn. Det samme gjelder for aktivister eller statlige aktører.

Et element som gjerne vurderes når man skal definere trussel mot sine verdier, er hvor attraktive verdiene selskapet har er, relativt til andres verdier.

Billedlig forklart menes her at om Per har 10 kroner liggende åpent tilgjengelig i en park, vil en trusselaktør trolig heller ta Olas 100 kroner som ligger ved siden av. Det motsatte kan være tilfelle om Ola har vakthold på sine 100 kroner.

4.4 Sårbarhet

Verdier som utsettes for en trussel har forskjellig grad av sårbarhet for denne trusselaktøren. Man må derfor forstå hvilke barrierer man har, og hvilke barrierer man kan implementere, for å redusere egen sårbarhet. Slike barrierer kan være menneskelige, tekniske eller organisatoriske. Summen av barrierer som skal avskrekke, avdekke, forsinke eller være en respons til en trussel, må fungere sammen i et system for å oppnå ønsket effekt. Det betyr eksempelvis at kameraer, vakter og gjerder (fysisk sikkerhet) skal fungere sammen med datasikkerhet (informasjonssikkerhet) og bakgrunnssjekk av egne ansatte (personellsikkerhet).

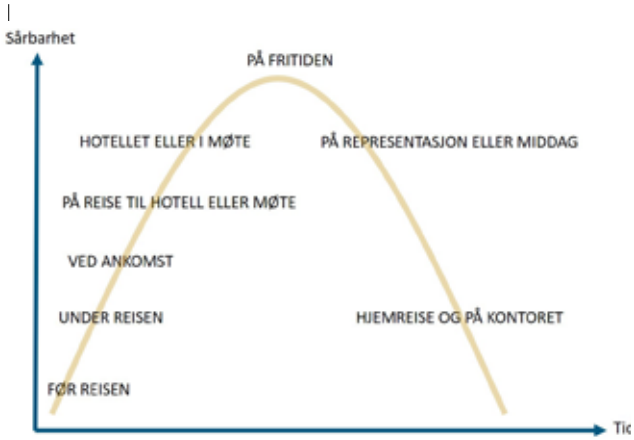
5. Forberedelser av ansatte

5.1 Reisesikkerhet

Forut for, og etter at virksomheten har etablert seg i utlandet, vil det være nødvendig å reise til og fra landet en har etablert seg i. I forbindelse med slike reiser kan det være mange forskjellige risikoer en kan bli utsatt for. Det kan være nyttig å gjennomføre egen opplæring i reisesikkerhet, med fokus på planlegging av reisen, risikovurdering av reisen og hvordan håndtere situasjoner en kan bli utsatt for.

I dagens teknologiske samfunn må det etableres gode rutiner for digital reisesikkerhet. Ofte reiser virksomhetens ansatte til utlandet med smarttelefoner, nettbrett og PC-er fulle av informasjon som lett kan kompromitteres om en ikke tar nødvendige forholdsregler. Derfor er det viktig å være forberedt på den økte risiko reisevirksomhet fører med seg.

«Veileder i reisesikkerhet» utgitt av Næringslivets Sikkerhetsråd i 2019.



5.2 Forventningsavklaring

Det kan være stor forskjell på å bo i Norge og i utlandet. Hjemme i Norge kjenner vi alle kodene i samfunnet. I utlandet kan dette være annerledes. Derfor er det viktig å ha en forventningsavklaring når det gjelder hva de utstasjonerte kan gjøre og hva de ikke kan gjøre. Herunder, hvordan kan de utestasjonerte forflytte seg? Tillates det for eksempel å benytte offentlig transport? Hvordan skal de utstasjonerte bo, og hvilke krav stiller virksomheten til sikring av boligen? Kan de utstasjonerte oppholde seg hvor de vil eller vil virksomheten sette begrensninger for hvor en kan oppholde seg?

Husk at virksomhetens utstasjonerte er der for å gjøre en jobb. Det er investert betydelig i de ansatte og det vil koste virksomheten mye å erstatte en ansatt dersom utstasjoneringen må avbrytes. Virksomheten er ansvarlig for den utsasjonerte 24/7-365 og bør stille krav til hva han eller hun kan gjøre – også i «fritiden». Derfor er det virksomheten som bør bestemme om man kan få lov til å kjøre bil selv, eller om man kan bruke for eksempel privat båt utenfor arbeidstiden. Rettigheter og begrensninger for medfølgere (familie osv.) til utstasjonerte bør defineres og klargjøres på et tidlig tidspunkt, på lik linje som for den ansatte. Tiltak må baseres på en risikovurdering.

6. Anbefalte tiltak

Lokale skikker, kultur og lignende må forstås. Sikkerhet i utlandet starter med kulturell forståelse. En viktig pekepinn på hvordan en skal opptre i utlandet er å rådføre seg med de lokalt ansatte. Det tar tid å lære seg kultur, selv etter å ha vært der i årevis.

Rapportering av sikkerhetshendelser slurves det noen ganger med. Virksomheten bør etablere et system hvor alle sikkerhetsrelaterte hendelser rapporteres internt i landet og til Norge. Dette må gjøres for at virksomheten kan danne seg et helhetlig bilde av risiko. Det bør for eksempel også være en årlig gjennomgang av rapporterte hendelser mellom sikkerhetsleder og virksomhetens ledelse. Eksempler på sikkerhetshendelser som bør rapporteres er tyveri (for eksempel mobiltelefoner, PC-er, produkter, biler), innbrudd (bolig, også til lokalansatte, kontor, produksjonsfasiliteter), kidnapping, ran, informasjonstyveri/kompromitteringer og utpressing.

Beredskaps- og kontinuitetsplaner er viktige forutsetninger for å lykkes når en hendelse inntreffer. Sørg for at det utarbeides slike planer, og at de som skal håndtere hendelser er trent i rolle og har øvd på relevante scenarioer. Det bør være en rød tråd i beredskaps- og kontinuitetsplanene som er utarbeidet i Norge og utlandet, slik at det blir enklere å samhandle når en har behov for det. Dersom virksomheten har en avtale med for eksempel den lokale utenriksstasjonen, Sjømannskirken eller andre aktører kan det være en god idé å involvere disse både i planlegging, trening og øving.

Cybertrusselen er høy de fleste steder. Et cyberangrep kan, dersom det ikke blir håndtert på en god måte, være ødeleggende for virksomheten. Derfor er god sikkerhetskultur et forebyggende tiltak. Andre tiltak kan være cyberpolicy, styringssystem, klare roller og ansvar, trening, opplæring og øvelser, cyberkompetanse, responsplaner og forhåndsavklarte kontaktpunkt med relevante myndigheter.

Kontorfasilitetene er gjerne det første virksomhetens gjester møter når de besøker virksomheten i utlandet. Sørg for at det etableres et system for adgangskontroll og registrering av besøkende, og at det etableres soner avhengig av hvilken informasjon eller aktivitet som utføres på kontoret. Besøkende bør eksponeres for minst mulig av den skjermede aktiviteten uten at virksomheten fremstår som lukket og utilgjengelig.

Transport av personell og varer gjør virksomheten sårbar. Det er viktig å gjennomføre risikovurderinger for all transport. For eksempel hvem som bør transportere virksomhetens ansatte og varer, til hvilke tidspunkter og langs hvilke transportruter. Tyveri av produkter under transport er et velkjent problem som virksomheter bør finne en løsning på. Sørg derfor for å etablere gode rutiner for all type transport, og at de som utfører slike oppgaver for virksomheten har alle tillatelser og sertifikater i orden. Er det for eksempel mulig å gjennomføre bakgrunnssjekk av sjåfører?

Produksjonsfasiliteter har vanligvis få besøkende utenom de som har sitt daglige arbeid der. Derfor er det viktig å sørge for at de som jobber der får utføre jobben sin uten å bli forstyrret av utenforstående og at eventuelle virksomhetshemmeligheter blir beskyttet. Dette gjøres enklest ved å etablere gode rutiner for adgangskontroll og soneinndeling.

Lagre er ofte interessante for kriminelle fordi her finnes det enten produksjonsmateriell, reservedeler, verktøy eller ferdige produkter som alle har verdi og ofte er lett omsettelige. Sørg for å etablere gode rutiner for inn- og utlevering fra lagre. Ha effektiv adgangskontroll.

7. Råd og tips

7.1 Bistand, hjelp og råd

Næringslivets Sikkerhetsråd kan bistå virksomheter som ønsker å etablere seg i utlandet med å komme i kontakt med medlemsbedrifter som har lang erfaring med dette. Slik bistand kan organiseres av Næringslivets Sikkerhetsråd enten i form av seminarer og konferanser eller bilaterale møter virksomheter imellom.

Norske utenriksstasjoner som ambassader og konsulater kan være en nyttig kilde til informasjon om lokale forhold. Samtidig kan de være behjelpelig med nettverk mot andre norske virksomheter i landet, og derigjennom dele informasjon og erfaringer. Ved behov kan norske utenriksstasjoner bistå med konsulær bistand til norske borgere i utlandet. Dersom virksomheten har ansatte som ikke er norske borgere, bør virksomheten identifisere disse landenes utenriksstasjoner, og hvordan disse kan bistå sine lands borgere.

Sjømannskirken er en selvstendig og frivillig organisasjon som på vegne av Den norske kirke skaper sosiale og kulturelle møtesteder, og er kirke for nordmenn i utlandet. Sjømannskirken finnes på alle kontinenter og har spesialkompetanse på kriseberedskap. Norske virksomheter som ønsker å benytte seg av Sjømannskirkens tjenester bør lage en egen skriftlig avtale om bistand og samhandling.

7.2 Leverandører av sikkerhetsinformasjon

Virksomheter som har aktivitet i utlandet har gjerne behov for oppdatert sikkerhetsinformasjon. Virksomheten bør vurdere å ansette en sikkerhetsleder for å strukturere dette arbeidet. Alternativt kan virksomheten vurdere å knytte seg opp mot en av de globale profesjonelle aktørene i markedet.

Globale sikkerhets- og rådgivingsselskaper tilbyr ofte abonnementsløsninger hvor det er mulig å skreddersy sikkerhetsinformasjon til det virksomheten har behov for. Samtidig har de ofte regionale eller lokale kontorer som kan hjelpe til med rådgivning, innhenting av spesiell informasjon eller utarbeiding av rapporter.

Lokale sikkerhetsselskaper er nyttige å knytte seg til fordi de ofte har god kunnskap om lokale utfordringer, ofte bedre enn de store globale selskapene. De kan også benyttes til resepsjonstjenester, sjåførtjenester og generelt vakthold av virksomhetens aktiviteter (boliger, kontorer, produksjonsfasiliteter, logistikk o.l.). Lokale sikkerhetsselskaper er ofte undervurdert, men de kan være en viktig kilde til informasjon og bistand. Erfaringsmessig er det nyttig å ha en kombinasjon av regionale og lokale kilder for å se hele bildet.

Væpnede vakter er ofte benyttet i mange land rundt om i verden. Virksomheten må vurdere om de egentlig trenger denne tjenesten. Deretter må virksomheten gjøre seg kjent med hvilket legalt ansvar en påtar seg når en leier inn væpnede vakter. Ofte tiltrekker væpnede vakter seg mer negativ oppmerksomhet enn den positive effekten av væpnet vakthold. Derfor må det ligge en grundig vurdering bak avgjørelsen om å benytte væpnede vakter. Flere store norske selskaper som benytter væpnede vakter må ha godkjennelse av konsernledelse forut for å bruke denne tjenesten.

Publisert:
November 2019

Trykk:
ETN Grafisk

Layout og illustrasjoner:
Næringslivets Sikkerhetsråd

Foto:
Adobe Stock/Arne Røed-Simonsen

Kontakt:
E-post: nsr@nsr-org.no

Adresse:
Middelthuns gate 27, Majorstuen

Notater

www.nsr-org.no

Næringslivets sikkerhetsråd

Mot kriminalitet - for næringsliv og samfunn