NVE

VEILEDER NR. 1 / 2024

Veileder i personellsikkerhet for kraftforsyningen

SKREVET AV Advansia

NVE Veileder nr. 1/2024
Veileder i personellsikkerhet for kraftforsyningen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Mari Bondevik
Forfatter:	Advansia
Omslagsbilde:	Kraftledningsmast på Ulriken i Bergen. Foto: Bjørn Lytskjold/NVE

ISBN (trykt utg.):	978-82-410-2346-0
ISBN (online):	978-82-410-2347-7
ISSN (trykt utg.):	1501-0678
ISSN (online):	2704-0356
Saksnummer:	202400229

Sammendrag: Veilederen søker å bistå virksomhetene i kraftforsyningen med konkrete tiltak som kan minske risikoen for innsiderisiko. Den er et resultat av samtaler med et utvalg ulike virksomheter i kraftforsyningen. Samtalene omhandlet i stor grad hvordan virksomhetene jobber med personellsikkerhet og hvilke utfordringer de møter på.

Emneord: Personellsikkerhet, Innsiderisiko, Innsidetrussel, Kraftforsyning, Sikkerhetsstyring, Kraftberedskapsforskriften,Risiko, Personalledelse

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

Januar 2024

Forord

Kraftforsyningen forholder seg daglig til krav og retningslinjer for fysisk og digital sikring. Kraftberedskapsforskriften har i mindre grad hatt fokus på personellsikkerhet. Menneskene er vår viktigste ressurs og de fleste medarbeidere vil i løpet av arbeidsforholdet havne i situasjoner eller bli utsatt for hendelser som kan påvirke motivasjon og lojalitet. Under det gjeldende trusselbildet har personellsikkerhet fått ekstra aktualitet.

Ivaretakelse av medarbeidere og minimering av innsiderisiko går hånd i hånd. Tiltakene må være preget av åpenhet og tett oppfølging av den enkelte medarbeider. Sikkerhetsmessig vil tiltakene være både av teknisk, menneskelig og organisatorisk art. Tydelig ledelse, utvikling av sikkerhetskultur, gode rutiner for sikkerhetsstyring og anvendelige verktøy for personal- og linjeledelse er viktige elementer.

Vi vil takke Advansia, som har utarbeidet veilederen, samt alle virksomhetene som stilte opp i intervjuer og har bidratt med uvurderlig kunnskap om utfordringer og mulige løsninger.

Virksomhetene som ble intervjuet er: Aneo, Trønder Energi, Linea, Helgeland Kraft, Lnett, Lyse, Arva, Tensio, Elvia, Barents Nett, BKK og Hafslund Eco.

Oslo, 9. januar 2024

Eldri Naadland Holo
seksjonssjef
Seksjon for beredskap
Tilsyns- og beredskaosavdelingen

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Innhold

1 Innledning

1.1 Bakgrunn

Norges vassdrags- og energidirektorat (NVE) har det nasjonale ansvaret for å forvalte landets vann- og energiressurser, herunder å sørge for sikker kraftforsyning. Kraftsystemene i Norge er en av de viktigste infrastrukturene vi har for å sikre kritiske samfunnsfunksjoner. Sikkerhet i alle ledd i hele kraftforsyningskjeden er derfor helt avgjørende.

Kraftforsyningen i Norge er kompleks og består av mange virksomheter med stor variasjon, både når det gjelder størrelse og organisatorisk innretning, geografisk beliggenhet og hvilken funksjon de har i forsyningskjeden. Dette medfører at virksomhetene har ulike forutsetninger, utfordringer, erfaringer og behov for kompetanse i sikkerhetsrelaterte spørsmål.

For å ivareta de ulike behovene, og med bakgrunn i den sikkerhetspolitiske situasjonen som utspiller seg, ser NVE det som formålstjenlig å utvikle en egen veileder i personellsikkerhet for kraftforsyningen.

Anbefalinger og forslag til tiltak som kommer frem i veilederen må ses som et tillegg til, og ikke som en erstatning for, krav hjemlet i kraftberedskapsforskriften. I spørsmål der andre lover vil kunne komme til anvendelse må det gjøres individuelle vurderinger.

Veilederen vil ikke kunne gi konkrete løsninger i det som ofte er komplekse problemstillinger og berører ulike lover og forskrifter. Veilederen vil først og fremst være et nyttig og praktisk hjelpemiddel for refleksjoner og tilnærming til spørsmål om personellsikkerhet.

For å lykkes best mulig bør arbeidet med personellsikkerhet ha en helhetlig tilnærming og være en integrert del av virksomhetens øvrige arbeid med sikkerhet. Det betyr at personellsikkerhet, IKT-sikkerhet og fysisk sikkerhet må ses i sammenheng, slik at de ulike menneskelige, teknologiske og organisatoriske tiltakene får gjensidig forsterkende effekt.

1.2 Formål

Personellsikkerhet handler om å implementere tiltak som reduserer risikoen for at ansatte utgjør en sikkerhetsrisiko, med andre ord redusere risikoen for innsidevirksomhet. Veilederen er ment som et støttedokument for å legge til rette for en tilnærmet lik og beste praksis.

Veilederens formål er å beskrive *hvordan* virksomhetene i kraftforsyningen kan arbeide systematisk med personellsikkerhet i de ulike fasene av et ansettelsesforhold. Dette arbeidet starter allerede tidlig i en rekrutteringsprosess og pågår helt til arbeidsforholdet opphører.

2 Sikkerhetsstyring

Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for at man beskytter sin virksomhet mot tilsiktede uønskede handlinger. Sikkerhetsstyring bør være en del av det overordnede styringssystemet til virksomheten.[i] For at virksomheter i kraftforsyningen skal kunne håndtere sårbarheter som mennesker kan utgjøre, er det viktig at arbeidet med personellsikkerhet er en integrert del av styringssystemet for sikkerhet og virksomhetens totale risikostyring.

Alle ansatte har et ansvar for å støtte opp om sikkerhetsarbeidet, men noen roller er mer sentrale. Det er viktig at disse rollene og ansvaret er tydelig definert og kjent i virksomhetene.

Utover en sikkerhetsleders ansvar for å systematisere og koordinere det forebyggende sikkerhetsarbeidet, vil ledere med personalansvar ha et særskilt ansvar for å følge opp ansatte gjennom den daglige sikkerhetsmessige styringen. HR vil ha et særlig ansvar knyttet til rekruttering, herunder sikre at bakgrunnssjekk blir gjennomført, og beredskapsledere et særlig ansvar blant annet knyttet til hendelseshåndtering. Samspill og kunnskap om hverandres ansvarsområder er en forutsetning. Dette bidrar til en helhetlig ivaretagelse av tiltak og vil samlet sett styrke personellsikkerheten i virksomheten.

Verdivurdering

Hvilke tiltak som er aktuelle å iverksette må tilpasses virksomhetens verdier og hva den skal beskytte. En helt sentral del av sikkerhetsstyringen er derfor å gjennomføre en verdivurdering for å få en oversikt over de viktigste verdiene, hvilket igjen vil kunne bidra til en mer fornuftig bruk av ressurser på sikkerhet.

Flere virksomheter i kraftforsyningen har gode rutiner for kartlegging og vurdering av sentrale verdier i virksomheten. Blant disse inngår den operative driften av anleggene, tilgjengelighet for driftskontroll- og IKT-systemer, den sikkerhetsmessige overvåkningen av anleggene og evnen til å håndtere ulike forsyningskritiske situasjoner.

I en slik vurdering må virksomhetene definere hvilke verdier som understøtter de sentrale leveransene og prosessene som er essensielle for egen drift. Deretter må det vurderes hva konsekvensene vil kunne være dersom verdiene ødelegges eller fjernes.[ii]

Sikkerhetskultur

Sikkerhetskultur kan beskrives som et sett med verdier som deles av medarbeidere i en virksomhet, og som – gjennom adferd og holdninger – er med på å påvirke deres tanker og forventninger til sikkerhet.[iii] «God sikkerhetskultur er når alle i en organisasjon har et bevisst og aktivt forhold til sikkerhet».[iv] Kontinuerlig arbeid med ulike tiltak over tid er en forutsetning for å bygge god sikkerhetskultur. Disse tiltakene systematiseres gjennom et godt styringssystem for sikkerhet. Tiltakene kan variere fra administrative tiltak som tydelige interne retningslinjer og instrukser, til tiltak som øker bevisstgjøringen og kompetansen om sikkerhet, som for eksempel opplæring av ansatte.

Et aktivitetshjul kan være en effektiv måte å organisere interne aktiviteter på som regelmessig skal gjennomføres. Videre bør sikkerhetstilstanden i virksomheten vurderes regelmessig. Gjennomfør regelmessige undersøkelser, vurderinger eller revisjoner av sikkerhetstilstanden relatert til personellsikkerhet. Her kan man identifisere områder for forbedring og bekrefte at retningslinjer blir etterfulgt.

En sentral del av en god sikkerhetskultur er en god rapporteringskultur.[v] Dette innebærer blant annet å oppfordre de ansatte til å rapportere om feil, avvik og andre type hendelser som er relevante for virksomheten. God rapporteringskultur er avgjørende for å kunne iverksette forbedringstiltak. I forbindelse med personellsikkerhet bør det legges til rette for varsling og rapportering av bekymringer på en diskré måte. Det er viktig at de ansatte er trygge på at rapportering ikke vil ha negativ konsekvens for den som rapporterer.

Uavhengig av hvilke tiltak som iverksettes er informasjon og kunnskap helt avgjørende for at tiltak blir forstått, gjennomført og etterlevd. Informasjon til ansatte, partnere, underleverandører, kandidater i en ansettelsesprosess og andre er med på å skape aksept, forståelse, motivasjon og bevissthet rundt personellsikkerhetstiltakene som virksomheten har iverksatt eller skal iverksette. I tillegg kan det gi større effekt av arbeidet med sikkerhetskultur om virksomheten utarbeidet systemer for å anerkjenne positiv sikkerhetsatferd. Dette kan bidra til å motivere ansatte til å ta sikkerhet på alvor og ikke være engstelige for å melde fra om hendelser.

Jobbtilfredshet

Trivsel på arbeidsplassen er viktig av flere årsaker, også for den forebyggende sikkerheten i en virksomhet og særlig for forebygging av innsidevirksomhet. Manglende jobbtilfredshet kan øke risikoen for innsidevirksomhet.[vi]

Sikkerhetsarbeidet skal ikke handle om mistenkeliggjøring av medarbeidere, men bør være rettet inn mot ivaretakelse av ansatte. Ansatte som ikke føler seg ivaretatt av arbeidsgiveren sin blir lettere misfornøyde. Misfornøyde ansatte, eller tidligere ansatte som av ulike årsaker bærer nag til arbeidsgiveren, kan ha et ønske om å ta hevn, for eksempel gjennom handlinger som kan ha negativ påvirkning eller skade sin nåværende eller tidligere arbeidsgiver. Det er derfor viktig å kartlegge nærmere hva som leder til jobbtilfredshet og/eller misnøye i virksomheten, herunder etablere prosesser eller verktøyer som måler ansattes tilfredshet, og hvordan eventuell misnøye kan endres og utvikles i en positiv retning. Dette eksisterer det mye forskning på, som kan benyttes.

Fokus på sikkerhetskultur og jobbtilfredshet vil være av spesiell viktighet i endrings-prosesser man antar kan lede til misfornøyde ansatte som f.eks. større organisasjons-endringer, oppkjøp, sammenslåinger m.m.

For å oppsummere dette kapittelet kan man si at sammenhengen mellom virksomhetens sikkerhetsstyring, sikkerhetsledelse, sikkerhetskultur, den enkeltes jobbtilfredshet og sikkerhetsbevissthet gjensidig påvirker hverandre. Dette må jobbes med og utvikles kontinuerlig.

2.1 Risikovurderinger

Sikkerhetsmyndighetene signaliserer i dag en tydelig forventning om at norske virksomheter tar grep for å ivareta sikkerheten. Risikovurderinger og sikkerhetstiltak må revideres oftere i takt med et stadig endret risikobilde. Dette gjelder også for virksomheter som ikke er underlagt sikkerhetsloven.[vii]

Kraftberedskapsforskriften § 2-3 pålegger alle KBO-enheter å gjennomføre risiko-vurderinger knyttet til ekstraordinære forhold. En oversikt over uønskede hendelser som skal innrapporteres til beredskapsmyndigheten er listet opp i kraftberedskapsforskriften § 2-6, og innebærer hendelser forårsaket av teknisk svikt, naturgitt skade og tilsiktede handlinger.

I et forebyggende personellsikkerhetsperspektiv anbefales virksomheter i kraftforsyningen også å gjennomføre risikovurderinger utover ekstraordinære forhold, eksempelvis ved tjenesteutsetting, innleie, anskaffelser og ansettelser. Herunder bør man særlig være oppmerksom på tjenester og ressurser som blir levert fra utlandet.

Risikovurderingene bør være kunnskapsbaserte og verdisentriske. Med verdisentrisk i denne sammenheng menes at verdiene som er viktige og kritiske for virksomheten er kartlagt som beskrevet under avsnittet «Verdivurdering» og gir føringer for den videre risikovurderingen. Videre bør de nasjonale åpne trusselvurderingene fra EOS-tjenestene (etterretnings-, overvåkings- og sikkerhetstjenestene), samt KraftCERT sin trusselvurdering legges til grunn. I tillegg kan det være nyttig å gjøre seg kjent med andre sektorvise eller lokale trusselvurderinger (for eksempel fra politidistrikter).

Når det gjelder tjenesteutsetting av IKT-tjenester fra andre land anbefaler NSM å særlig vurdere fire forhold:[viii]

1. Statlige styringsindikatorer.
2. Cybersikkerhetstilstanden i landet
3. IKT-infrastruktur og kompetanse i landet
4. Forretningsstabiliteten i landet.

For øvrig anbefaler NSM at alle beslutninger om tjenesteutsetting baseres på risikovurderinger som beskriver de faktiske risikoene tjenesteutsettingen medfører.[ix]

For å kunne vurdere disse forholdene må man benytte seg av tilgjengelig og oppdatert informasjon, samt identifisere relevante problemstillinger. Se vedlegg 1 for eksempler på kilder som kan være et godt hjelpemiddel i disse vurderingene.

God praksis knyttet til alle typer risikovurderinger handler altså først og fremst om å identifisere behov, samt gjennomføre og revidere vurderingene jevnlig for å sikre at tiltakene er tilstrekkelige.

En virksomhet i kraftforsyningen vil ha flere legitime grunner til å implementere personellsikkerhetstiltak både i kraft av å skulle ivareta samfunnskritiske funksjoner, men også for å ivareta kommersielle behov og interesser.

3 Trusselbildet

Trusselbildet i Norge er sammensatt, komplekst og endrer seg raskt. Russlands angrepskrig mot Ukraina er et godt eksempel på raske endringer i trusselbildet og hvordan dette brått forsterket og utløste nye sikkerhetsutfordringer for Norge. Et stadig endret trusselbilde vil føre med seg implikasjoner for personellsikkerheten i kraftforsyningen.

Flere lands etterretningstjenester opererer på norsk jord. Enkelte statlige aktører har svært stor evne til å gjennomføre etterretningsoperasjoner, og er villige til å ta stor risiko for å gjennomføre sine aktiviteter. Hensikten kan være å innhente informasjon som vil styrke egne militære, økonomiske eller strategiske kapasiteter, svekke, skade eller påvirke virksomheter i Norge, eller i verste fall forberede og gjennomføre sabotasjehandlinger.

Etterretningsaktivitet fra Kina, Russland og Iran har i flere år vært fremhevet av nasjonale sikkerhetsmyndigheter som den største etterretningstrusselen mot Norge. Kraftforsyningen og norsk infrastruktur er omtalt i de siste årenes trusselvurderinger som mål man forventer blir utsatt for etterretningsaktivitet.[x] Dette utelukker ikke at også andre land kan ha interesse av å gjennomføre etterretningsaktivitet mot Norge og forhold i norsk kraftforsyning.

Som en følge av den sikkerhetspolitiske situasjonen i Europa, har det tvunget seg frem en endring i *modus operandi* særlig for russiske sikkerhets- og etterretningstjenester. Samhandlingsarenaer har blitt begrenset som en følge av sanksjonsregimet, et stort antall etterretningsoffiserer tilknyttet den russiske ambassaden er utvist og det utvises generelt økt årvåkenhet i samfunnet. Dette betyr at arbeidsforholdene til etterretnings-offiserene har blitt vanskeligere, og de er avskåret fra å hente inn informasjon gjennom tidligere åpne kanaler. Deres informasjonsbehov er imidlertid større enn noen gang, noe som betyr at de må bruke andre metoder for å skaffe informasjon.

I lys av dette vil derfor cybertrusselen og innsidetrusselen kunne øke for å erstatte innhentingsmetoder som krever fysisk nærvær av eget etterretningspersonell.

Rekruttering av kilder og kontakter vurderes å være en særlig prioritert oppgave for etterretningstjenester i tiden fremover, og de beste kildene vil være de som har tilgang til verdier fra innsiden av en virksomhet. Ved å ha en innsider i virksomheter i kraftforsyningen vil de kunne få unik og sensitiv informasjon om blant annet ansatte, rutiner, sikkerhetstiltak og infrastruktur som på et senere tidspunkt kan utnyttes.

Innsidevirksomhet kan også være drevet av ikke-statlige aktører og organiserte kriminelle med høy kapasitet, eller lavkapasitetsaktører i form av opportunister med mer kortsiktige mål. Hensikten vil kunne være sabotasje/skadeverk, svindel eller industrispionasje med mål som for eksempel driftsforstyrrelser eller avbrudd, økonomisk vinning eller posisjonering i kraftmarkedet. Ved å ha en innsider i kraftforsyningen vil man blant annet kunne skaffe seg kunnskap om infrastruktur, tilgang til sensitiv informasjon, eller tilegne seg fordeler i eierskap og oppkjøpsprosesser. Aktørene vil kunne benytte seg av metoder som i mange tilfeller er sammenfallende med statlige aktører, og en innsider vil derfor være svært attraktiv.

4 Innsidetrusselen

Kunnskap om trusler er en viktig faktor i det forebyggende sikkerhetsarbeidet. Ved å identifisere relevante trusselaktører som har eller kan få intensjon om å skade kraftforsyningen i Norge vil man være i bedre stand til å kunne velge riktige sikringstiltak. Kunnskap om innsidetrusselen er intet unntak. Dette er imidlertid et komplekst fenomen, og kan derfor ikke vurderes som en homogen aktørgruppe.

Det finnes ingen universell definisjon av begrepet innsider, men en definisjon som ofte benyttes nasjonalt er hentet fra Nasjonal sikkerhetsmyndighet (NSM):

> *«En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen til å utføre handlinger som påfører virksomheten skade eller tap.»*

Innsiderisiko er som nevnt komplekst og oppleves ofte som svært utfordrende å håndtere. Dette henger sammen med at trusler fra innsiden er vanskelig å oppdage og forhindre fordi den utøves av personell med lovlige tilganger. Dette er mennesker som er gitt tillit, kjenner organisasjonen godt, kan omgå sikkerhetsbarrierer og operere i det skjulte. I tillegg består innsidetrusselen av mennesker som drives av ulike motiv, noe som igjen vil kreve ulike forebyggende tiltak.

Av åpenbare grunner er det vanskelig å finne sikker statistikk over innsiderisiko, men ifølge Næringslivets sikkerhetsråds Kriminalitets- og sikkerhetsundersøkelse i Norge (KRISINO) fra 2021 har 8 prosent av de deltagende norske virksomhetene avdekket utro tjenere. 88 prosent vet ikke eller anser det som ikke aktuelt.[xi] Handlingene dreier seg om alt fra CV-juks, underslag og tyveri, til hærverk eller sabotasje, lekking av informasjon og industrispionasje. Mørketallene er trolig store, men statistikken vitner uansett om at innsidetrusselen er høyst reell. Innsiderisiko i kraftforsyningen kan blant annet medføre økonomiske tap, tap av omdømme, kompromittering av kraftsensitiv informasjon, driftsforstyrrelser og i ytterste fall få alvorlige konsekvenser for kritiske samfunnsfunksjoner.

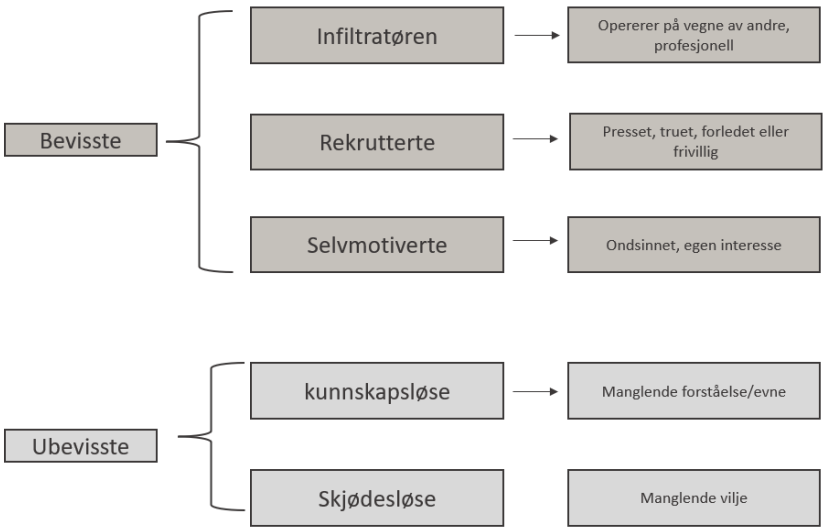
Det er verdt å merke seg at det finnes både bevisste og ubevisste innsidere.

En *bevisst innsider* er en person som har intensjon om å utnytte og/eller skade virksomheten, enten på egne eller andres vegne.

En *ubevisst innsider* er en person som i utgangspunktet er uten intensjon om å utnytte og/eller skade virksomheten. Dette er gjerne personer som uaktsomt eller tilfeldig påfører virksomheten skade eller tap, og henger ofte sammen med lav sikkerhetsmessig bevissthet eller neglisjerende holdninger til å følge regelverk og instrukser.

Ifølge Insider Threat Detection study (NATO)[xii] er ubevisst innsidevirksomhet mer vanlig en bevisst. Skadepotensialet anses mindre sammenlignet med målrettede bevisste handlinger, men vil potensielt kunne få svært negative konsekvenser.

Kategoriene av innsidere *kan* visualiseres på denne måten:



Kilde: Advansia. Det eksisterer flere ulike benevninger og inndelinger på innsidekategorier. Modellen er en forenklet sammenstilling av de ulike innsidekategoriene som beskrives av både nasjonale og andre lands sikkerhetsmyndigheter og organisasjoner

I de følgende avsnittene er hensikten å gi en mer utfyllende beskrivelse av de ulike kategoriene innsidere; hvem de er, hvorfor de handler som de gjør, hvordan menneskelige sårbarheter utgjør en risiko og i hvilken grad det er mulig å gjenkjenne eller få forhåndsvarsel på innsidere.

NB! Definisjonene er i endring
I henhold til trefaktormodellen (hvor faktorene er risiko, trussel og sårbarhet) er en ubevisst innsider snarere å forstå som en sårbarhet for virksomheten, heller enn en trussel. En mer konsistent terminologi er å si at en enhver person eller gruppe med autorisert tilgang eller kunnskap om virksomhetens verdier er en innsider.

***Innsiderisiko** handler om skade eller tap for en virksomhet på grunn av innsiderens adferd, og ulik adferd kan generelt være aktive handlinger, uaktsomhet eller passivitet.*

*En **innsidetrussel** er spesifikt en person (eller gruppe) drevet av en intensjon om skade eller tap.*

*En **innsidehendelse** er resultat av adferd som søker eller forårsaker skade eller tap for virksomheten.*

Britiske NPSA endret definisjonen av innsider i 2023, og trolig vil også de benyttede norske definisjonene med tiden bli justert.

4.1 Innsidekategorier

4.1.1 Bevisste

En *bevisst innsider* er en person som har intensjon om å utnytte og/eller skade virksomheten, enten på egne eller andres vegne. Bevisste innsidere deles ofte inn i tre underkategorier; infiltratører, rekrutterte og selvmotiverte.

Infiltratøren

Infiltratøren er den profesjonelle innsideren. Vedkommende er gjerne utdannet i etterretningsfaget og opererer på vegne av en organisasjon eller fremmed stats etterretningstjeneste.

Infiltrasjonen er en styrt investering og har lang planleggings- og tidshorisont. Vedkommende kan bruke mange år på å bygge opp en falsk identitet og tilegne seg nødvendig fagkunnskap for stillingen man besitter eller er tiltenkt. Infiltratøren omtales også som illegalist eller agent under dekke.

Motivet til infiltratøren er rett og slett å utføre jobben sin. Oppdraget kan for eksempel være å hente ut informasjon, påvirke beslutningsprosesser, skade infrastruktur eller tilrettelegge for at andre kan gjennomføre skadelige handlinger på et senere tidspunkt.

Infiltratørens profesjonalitet gjør at denne kategorien innsidere er særlig vanskelig å forebygge og avdekke gjennom forebyggende tiltak, som bakgrunnssjekk eller gjennom bekymringsfull adferd. Det er lagt ned store ressurser i å lage troverdige dekkhistorier, ID dokument og CV. Infiltratøren vil ha svært gode sosiale egenskaper og tilpasser seg arbeidsforholdene og kollegaer uten å vekke negativ oppmerksomhet.

Ifølge NPSA (tidligere CPNI)[xiii] utgjør denne kategorien en liten andel av kjente innside-saker.

Rekrutterte

Rekrutterte innsidere utfører innsidevirksomhet på vegne av andre, enten frivillig, under press eller fordi vedkommende er forledet. Vedkommende er i utgangspunktet uskolert i etterretningsfaget, men vil få opplæring og føringer fra sin oppdragsgiver. Den rekrutterte innsideren er ofte allerede ansatt i virksomheten som trusselaktøren ønsker informasjon fra, eller personen er i posisjon til å kunne bli det.

Rekrutteringsprosessen foregår gjerne fordekt og med lang tidshorisont. Kartlegging, målutvelgelse, tilnærming og relasjonsbygging kan forekomme både fysisk og digitalt, er nøye planlagt og oppfattes ikke nødvendigvis som forberedelser til et rekrutterings-forsøk. Tilnærmingen kan utføres av etterretningsoffiserer med dekkstillinger ved hjem-landets ambassader, men også av etterretningspersonell fordekt i andre stillinger eller posisjoner.

Kultivering i form av oppmerksomhet, invitasjoner, gaver eller andre goder forekommer og kan oppleves som en ufarlig og naturlig del av relasjonen. Prosessen bidrar til å kartlegge medarbeiderens potensiale og kan senere benyttes til å skreddersy den påfølgende rekrutteringsstrategien. Sårbarheter som avdekkes vil særlig kunne utnyttes. Relasjonsbygging over tid kan generelt bidra til å senke terskelen for samarbeid, eller medføre at man har satt seg i en form for gjeld eller blitt utsatt for kompromitterende situasjoner som brukes som pressmidler.

Autoritære og totalitære regimer respekterer ikke menneskerettigheter og andre demokratiske spilleregler. Dette kan blant annet gi seg utslag i krav og forventninger om at borgere av slike land må samarbeide med hjemlige myndigheter. Noen personer vil gjøre dette frivillig, andre blir truet og presset til det. Kinas etterretningslov av 2017, kan for eksempel kreve at kinesiske borgere i utlandet bidrar til å hente inn informasjon til myndighetene (artikkel 7).

Nordmenn på reise til høyrisikoland kan også bli utsatt for rekrutteringsforsøk. Med høyrisikoland menes her stater som Politiets sikkerhetstjeneste (PST) har angitt i sine åpne trusselvurderinger som stater det knytter seg særlig høy etterretningstrussel til. De stedlige etterretningstjenestene har videre fullmakter til overvåkning og utøvelse av press på hjemmebane og kan benytte dette til å utnytte personer i Norge.

Rekruttering av kilder kan forenklet visualiseres på denne måten:

Enhver ansatt kan bli utsatt for rekrutteringsforsøk. Enkelte ansatte vil imidlertid kunne være mer sårbare enn andre dersom de for eksempel har tilhørighet eller tilknytning til høyrisikoland, innehar nøkkelfunksjoner eller stillinger av stor etterretningsmessig verdi, eller befinner seg i en vanskelig livssituasjon. I den grad det er mulig bør dette kartlegges i rekrutteringsfasen og ivaretas kontinuerlig gjennom daglig sikkerhetsmessig styring med relevante forbyggende tiltak.

Selvmotiverte

Selvmotiverte innsidere er drevet av egne interesser og bevisste valg. Denne kategorien innsidere kjennetegnes av et stort spenn knyttet til bakenforliggende og utløsende motiv, for eksempel:

- Økonomi
- Ideologi
- Ønske om anerkjennelse
- Misnøye eller mistrivsel
- Behov for spenning
- Hevn
- Lojalitetskonflikt

Menneskers tanker, ideer og holdninger kan endre seg på både kort og lang sikt. Både personlighetstrekk, ytre stressfaktorer og organisatoriske svakheter kan være avgjørende for om denne kategorien innsidere faktisk begår ondsinnede handlinger. Dette understreker behovet for at alle ansatte ivaretas kontinuerlig gjennom daglig sikkerhetsmessig styring med relevante forbyggende tiltak.

4.1.2 Ubevisste

En *ubevisst innsider* er en person som i utgangspunktet er uten intensjon om å utnytte og/eller skade virksomheten. Dette er gjerne personer som uaktsomt eller tilfeldig påfører virksomheten skade eller tap. Ubevisst innsidevirksomhet henger ofte sammen med lav sikkerhetsmessig bevissthet eller neglisjerende holdninger til å følge regelverk og instrukser. Ubevisste innsidere er mer vanlig enn bevisste innsidere, og vil kunne utgjøre en betydelig risiko for virksomheter. Ubeviste innsidere er særlig utsatt for sosial manipulering.

Sosial manipulering (Social Engineering)

Angrep som benytter seg av psykologiske teknikker for å manipulere mennesker til å utføre spesifikke handlinger eller avsløre sensitiv informasjon. Trusselaktøren spiller gjerne på menneskelige følelser som frykt, fristelser, tillitt og tidspress.

Eksempler på angrepsflater: sosiale medier, e-post, tekstmeldinger, telefonsamtaler eller andre digitale kanaler.

Eksempler på angrepsformer: phishing, spear phishing, smishing, vishing.

Digitalisering og den raske teknologiske utviklingen gjør at angrepsmetoden blir stadig mer sofistikert og metoden benyttes av både statlige aktører og kriminelle.

Et målrettet cyberangrep kan for eksempel gjennomføres etter forutgående innhenting av informasjon gjennom sosial manipulering av ansatte. Et eksempel på dette er angrepet på Hydro i 2019.

Under følger en beskrivelse av de to kategoriene av ubevisste innsidere.

Kunnskapsløse

Den kunnskapsløse innsideren utsetter virksomheten sin for skade og/eller tap uaktsomt eller tilfeldig. Dette henger gjerne sammen med at vedkommende ikke har forståelse eller kunnskap om sikkerhetsmessige forhold.

Vedkommende har for eksempel liten forståelse av hvilken verdi kraftforsyningen har i et samfunnssikkerhetsperspektiv, kjenner ikke til det overordnede trusselbildet, mangler forståelse for egen rolle, kjenner ikke hva som er kraftsensitiv informasjon og hvordan dette skal forvaltes, eller mangler bevissthet om risiko.

Personlighetstrekk, ytre stressfaktorer og organisatoriske svakheter kan være avgjørende for om denne kategorien innsidere faktisk begår ubevisste skadelige handlinger. Det er derfor avgjørende at ansatte gis opplæring og kunnskap tidlig i rekrutteringsfasen og at dette følges opp kontinuerlig gjennom daglig sikkerhetsmessig styring med relevante forebyggende tiltak.

Skjødesløse

Den skjødesløse innsideren utsetter virksomheten sin for skade og/eller tap på grunn av uforsiktighet eller neglisjerende holdninger. Vedkommende har kunnskap om og forstår viktigheten av sikkerhetsanordninger, men velger å ignorere dette av ulike grunner, for eksempel:

- Stress og arbeidspress
- Velger å se det som irrelevant – «det gjelder ikke meg»

Også her kan personlighetstrekk, ytre stressfaktorer og organisatoriske svakheter være avgjørende for om denne kategorien innsidere materialiserer seg til skadelige handlinger.

Forebyggende tiltak overfor denne kategorien innsidere må særlig følges opp gjennom daglig sikkerhetsmessig styring med relevante forebyggende tiltak.

4.2 Menneskelige sårbarheter

Årsaken til at mennesker blir innsidere er som beskrevet mange og sammensatt, men en fellesnevner for flere av disse er menneskelige sårbarheter. Dette gjelder både de rekrutterte, de selvmotiverte og til en viss grad de ubevisste.

Menneskelige sårbarheter kan være medfødte egenskaper eller personlighetstrekk, eller sårbarheter utløst av ytre omstendigheter og påvirkning. For eksempel vil tilhørighet til høyrisikoland eller kriminelle gjøre ansatte sårbare dersom de blir utsatt for press, påvirkning eller forventninger om samarbeid. Ansatte vil også være mer sårbare dersom de befinner seg i en vanskelig livssituasjon, for eksempel utløst av høyt arbeidspress, dårlig økonomi, rusavhengighet, sykdom eller samlivsbrudd. Sammen med teknologiske og organisatoriske svakheter i en virksomhet kan dette samlet sett forsterke risikoen for innsidevirksomhet.

Modellen under visualiserer hvordan menneskelige sårbarheter utgjør en av flere faktorer i et større bilde. Det er viktig å understeke at disse indikatorene hverken hver for seg eller sammensatt er beskrivelse av en innsider-profil, men at dette er ment å gi kunnskap og forståelse om hva som i noen tilfeller kan lede til innsidevirksomhet.

Figur: Basert på Shaw and Seller`s critical pathway[xiv]

5 Systematisk arbeid med personellsikkerhet

Kraftforsyningen har særtrekk som skiller seg fra andre bransjer og som krever noen tilpasninger i det systematiske arbeidet med personellsikkerhet. Blant disse er utstrakt bruk av underleverandører og enkeltpersoner med vide adganger på forskjellige avsidesliggende anlegg. Disse eksemplene representerer ingen uttømmende liste, men er aspekter som bør hensyntas i arbeidet med personellsikkerhet.

5.1 DEL 1 - Rekrutteringsfasen

Tiltak i rekrutteringsfasen vil redusere risikoen for feilansettelser og identifisere sårbarheter hos kandidater som bør følges opp etter en eventuell ansettelse.

Tiltaksanbefalingene i rekrutteringsprosessen er utfyllende beskrevet under, i den rekkefølgen de bør gjennomføres. På slutten av kapittelet oppsummeres anbefalingene i form av en sjekkliste.

Etablere tverrfaglige sikkerhetsteam.

Om mulig bør det vurderes å etablere tverrfaglige team bestående av HR, sikkerhet, juridisk, og den fagenheten som ansetter. På den måten vil man sikre ulik kompetanse og at flere hensyn ivaretas i komplekse, og ofte juridiske, spørsmål i rekrutteringsprosesser. Personell med kompetanse innen personvernregelverket er avgjørende å involvere i sikkerhetsteamet.

Kompetansedeling øker kunnskap om de ulike behovene og kravene til ansettelsen/stillingen, samt forståelse og håndtering av innsiderisiko. Videre kan et tverrfaglig sikkerhetsteam styrke beslutningsgrunnlaget som utarbeides for ledelsen.

Sikkerhetsteamet bør være en gripbar ressurs i alt systematisk arbeid videre med personellsikkerhet.

Gjennomføre stillings -og prosjektspesifikke risikovurderinger

Før utlysning bør det gjennomføres en vurdering av den aktuelle stillingen eller prosjektet. Dette forutsetter kunnskap om hvilke verdier den aktuelle stillingen eller prosjektet vil gi tilgang til og hvilke konsekvenser innsidevirksomhet kan medføre. Disse vurderingene bør utføres av sikkerhetsteamet eller personell med tilsvarende kompetanse.

Dersom stillingen eller prosjektet er forbundet med forhøyet risiko, f.eks. stillinger som er nødvendig for å opprettholde forsyningssikkerhet (beredskaps- og lederpersonell, personell på driftssentraler, IT-personell, reparasjonspersonell mfl.) bør strengere krav eller kriterier for ansettelse vurderes og dokumenteres skriftlig i vurderingen.

En policy som beskriver eller definerer virksomhetens håndtering av søkere fra høyrisikoland bør defineres av virksomheten og inngå som del av styringssystemet for sikkerhet, samt implementeres hos HR/rekrutteringsansvarlige i virksomheten.

Her bør man støtte seg til EOS-tjenestenes trusselvurderinger og virksomhetens egne verdi- og risikovurderinger, for å vurdere hvorvidt hensynet til samfunnssikkerhet får betydning for kriterier for ansettelse. Dette bør være juridisk fundert og fremkomme skriftlig i vurderingen.

Utnytte utlysningstekstens muligheter

I denne delen av rekrutteringsprosessen bør man starte å alminneliggjøre fokuset på personellsikkerhet og innsiderisiko. I utarbeidelse av utlysningsteksten bør man benytte seg av formuleringer som viser at virksomheten setter sikkerhet høyt på agendaen, samt gjøre kandidaten kjent med at det vil bli gjennomført bakgrunnssjekk før en eventuell ansettelse. I utlysningsteksten kan det i visse stillinger være relevant å informere om at vedkommende i sin stilling kan få tilgang til kraftsensitiv informasjon og at man i rekrutteringsprosessen må påregne å svare på inngående spørsmål relatert til sikkerhet.

Fokus på sikkerhet kan signaliseres ved å informere om at man vektlegger personlig egnethet, lojalitet, god dømmekraft, evnen til å følge sikkerhetsanordninger m.m. Dette vil være momenter som naturlig kan følges opp i intervjuet og inngå som en del av egnethetsvurderingen. Dette kan ha avskrekkende effekt på søkere med uærlige hensikter eller som av andre grunner ikke anser seg egnet for stillingen.

Inkludere sikkerhet som tema i jobbintervjuet

Jobbintervjuet er en god arena for å få nødvendig informasjon og avklaringer knyttet til personellsikkerhet. Selv om det kan virke inngripende å stille spørsmål som gjelder sikkerhet, er det viktig at dette gjøres i rekrutteringsfasen.

Ved innkallingen av kandidater til intervju kan det være relevant å informere om at det vil bli stilt spørsmål knyttet til sikkerhet. Man kan for eksempel informere om at «virksomheten vår er underlagt kraftberedskapsforskriften. Sikkerhet vil derfor være en del av rekrutteringsprosessen hos oss og du vil måtte regne med å få spørsmål knyttet til personellsikkerhet».

Kandidatens CV bør gjennomgås under intervjuet. Hull i CV må kontrolleres og søkes avklart under intervjuet og ved egne undersøkelser.

Dersom sikkerhet har vært tydelig adressert i stillingsutlysningen vil det være en forventning og ikke en overraskelse for kandidaten når dette tas opp i intervjuet, noe som igjen vil bidra til at det oppleves mindre inngripende for begge parter. Videre er intervjuet også en fin anledning til å beskrive nærmere hvordan virksomheten jobber med sikkerhet i det daglige arbeidet. Dette vil i sum bidra til å alminneliggjøre temaet og bidra til økt forståelse for tiltakene.

Det bør stilles åpne og likelydende spørsmål til alle relevante kandidater. Dette vil være viktig med tanke på seleksjon og vekting videre i rekrutteringsprosessen. Særlig med tanke på vurdering av egnethet. Noen eksempler på åpne spørsmål som kan bidra til å belyse kandidatens syn på sikkerhet kan være:

- «Hva legger du i begrepet personellsikkerhet?»
- «Hvilke egenskaper tenker du er viktig for ansatte i en sektor som forvalter kritisk infrastruktur?»
- «Er det forhold du tenker at vi bør kjenne til for å kunne ivareta deg best mulig hvis du blir ansatt hos oss?»

Utføre ID-sjekk ved intervjuet

Bruk av falske identiteter er et stort problem. Falske, fiktive, stjålne eller lånte id-dokumenter benyttes til å søke jobb i både offentlig og privat sektor. Be kandidaten, uavhengig av landtilhørighet, om å ta med nasjonalt pass til intervjuet og til første arbeidsdag. Sjekk dokumentene nøye for å verifisere jobbsøkerens identitet.

Gjennomføre bakgrunnssjekk (og samtykke)

Ifølge kraftberedskapsforskriften § 6-7 om personkontroll skal bakgrunnssjekk gjennomføres i KBO-enheter ved nyansettelser eller egne ansatte som har fått ny stilling. Det er viktig å huske at man må ha samtykke, i henhold til personopplysningsloven.

Samtykket må være skriftlig og bør inneholde informasjon om hvem som gjennomfører bakgrunnssjekken, hensikt med tiltaket og hvordan resultatene benyttes, hvilken informasjon som verifiseres, hvilke kilder som kontaktes, rettigheter og personvernlovgivningen, samt hvor og hvordan opplysningene skal lagres.

En bakgrunnssjekk omfatter å innhente, sammenligne og dokumenter informasjon om kandidaten. Hensikten er å kunne bekrefte eller avkrefte informasjon som personen selv har oppgitt. I tillegg kan en bakgrunnssjekk virke avskrekkende og i så måte bidra til forebyggende sikkerhet i virksomheten.[xv]

En bakgrunnssjekk består i hovedsak av fire områder:

1. *Identitetskontroll (*ID bør sjekkes ved både intervju og oppstart)
2. *Verifikasjon av utdannelse og erfaring (*Benytt vitnemålsportalen og NOKUT)
3. *Sjekk av næringsinteresser (*Benytt f.eks. Brønnøysundregistrene)
4. *Søk i åpne kilder (*Søk i f.eks. sosiale media)

Bakgrunnssjekk er noe virksomheten kan utføre selv dersom det finnes kompetanse internt til å gjennomføre dette, eller man kan få bistand av en ekstern leverandør.

Eventuelle funn fra bakgrunnssjekken bør avklares i intervju. Hvis det åpenbarer seg utfordringer som ikke er forenlig med virksomhetens retningslinjer/rutiner for sikkerhet og verdier, bør virksomheten vurdere om ansettelse kan unngås.

En bakgrunnssjekk er et øyeblikksbilde av tilgjengelig informasjon. Den vil derfor aldri være noen garanti mot innsiderisiko, men i beste fall en forsikring om at opplysninger som er gitt i forbindelse med søknad og intervju stemmer.

Menneskers holdninger, tanker og ideer kan endre seg både på kort og lang sikt. Dette er forhold som ikke vil fanges opp av en bakgrunnssjekk, men som man må forsøke å fange opp i andre faser av ansettelsesforholdet.

Gjennomføre en selvstendig egnethetsvurdering

Ifølge kraftforsyningsforskriften § 6-7, femte ledd skal bakgrunnssjekk brukes som grunnlag for å vurdere en persons egnethet til å få tilgang til klassifiserte anlegg, system eller annet. Risikofaktorer som taler imot egnethet, er imidlertid forhold som ikke åpenbart avdekkes gjennom en bakgrunnssjekk. Det anbefales derfor at egnethetsvurderinger gjøres som en helhetlig og selvstendig vurdering. Denne bør inneholde funn/avklaringer fra bakgrunnssjekk, relevant informasjon som fremkommer i intervjuet og referansesamtaler samt eventuelt tilleggssøk i åpne kilder på nett.

CV'en er en viktig kilde til informasjon om kandidaten og bør kontrolleres. Et forhold er at informasjonen i CV'en kan være en forfalskning. Et annet forhold er at informasjon i CV kan indikere knytninger til hjemlandets militære eller etterretnings- og sikkerhetstjenester. Hull i CV'en bør undersøkes. Enkelte kandidater kan utelukke utdanning eller arbeidserfaring i CV'en for ikke å avsløre tilhørighet til hjemlandets myndighetsorgan.

Personopplysninger som behandles i forbindelse med egnethetsvurderingen skal slettes så snart formålet med innhentingen er oppfylt. Behandling av personopplysninger må gjøres i samsvar med personopplysningsloven.

Modellen under oppsummerer de overordnede stegene i rekrutteringsprosessen:

5.1.1 Oppsummerte anbefalte tiltak

Anbefalte tiltak i rekrutteringsfasen	
1	Etablere tverrfaglig sikkerhetsteam
2	Gjennomføre stillings- og prosjektspesifikke risikovurderinger
3	Utnytte utlysningstekstens muligheter
4	Benytte intervjuet til å stille spørsmål om sikkerhet, samt kontroll av ID
5	Gjennomføre bakgrunnssjekk
6	Gjennomføre egnethetsvurdering

5.2 DEL 2 - Daglig sikkerhetsmessig styring

Daglig sikkerhetsmessig styring refererer til det kontinuerlige arbeidet som gjøres innen sikkerhet, som planlegging, gjennomføring og monitorering av tiltak og etterlevelse. I et personellsikkerhetsperspektiv handler dette om å ivareta og følge opp ansatte med det formål å redusere innsiderisiko.

Tiltak knyttet til opplæring, kunnskap og bevisstgjøring er vesentlige i sikkerhetsledelse og -styring, herunder opplæring av ledere. Ledere er nøkkelpersonell i det forebyggende sikkerhetsarbeidet. De er rollemodeller og har ansvaret for å utføre daglig sikkerhetsmessig styring.

Det bør utarbeides en rutine for den innledende fasen av arbeidsforholdet. Rutinen bør inkludere administrative tiltak som er virksomhetsspesifikke, samt sikkerhetstiltak som for eksempel taushetserklæring, sikkerhetsinstruks, opplæring og kurs, varslingskanaler med mer. NVE har utarbeidet mal for taushetserklæring som kan benyttes av virksomheter i kraftforsyningen: mal-for-taushetserklæring.pdf (nve.no).[1]

Tiltaksanbefalingene i denne fasen er utfyllende beskrevet i den rekkefølgen de bør gjennomføres. På slutten av kapittelet oppsummeres anbefalingene i form av en sjekkliste.

Bakgrunnssjekk av ansatte ved endring av stilling

Når en ansatt søker seg til en annen stilling internt i virksomheten skal det gjennomføres bakgrunnssjekk, på lik linje som med nye ansatte. Det kan vurderes om det i tillegg bør

[1] NB! NVEs tilbudte mal omhandler spesifikt tilgang til kraftsensitiv informasjon. Vi anbefaler at virksomhetene lager egne maler for taushetserklæringer, eventuelt ved å benytte deler av innholdet fra NVEs mal.

gjennomføres en selvstendig egnethetsvurdering som beskrevet i kapittel 5.1 *Rekrutteringsfasen*.

Dette vil gi virksomheten en god anledning til å følge opp sine ansatte og være en påminnelse om fokuset virksomheten har på personellsikkerhet.

Gjennomføre obligatorisk oppstartssamtale med ID-sjekk

Gjennom en oppstartssamtale med nye ansatte bør man adressere personellsikkerhet og orientere om hvordan virksomheten jobber for å forebygge både bevisst og ubevisst innsidevirksomhet. Samtalen kan videre fungere som en viktig forventningsavklaring ved å informere om interne rutiner, prosedyrer, kurs og opplæring som virksomheten praktiserer. En slik samtale kan bidra til å unngå overraskelser, unødvendig mistenkeliggjøring eller stigmatisering på et senere tidspunkt dersom den ansatte for eksempel blir tilbudt en sårbarhetssamtale.

Husk at ID sjekk av den ansatte også bør gjøres ved oppstart, i tillegg til i intervjuet.

Etablere og gjennomføre obligatorisk introduksjonskurs/program

Personellsikkerhet og innsiderisiko bør være på agendaen når ansatte gjennomfører introduksjonskurs.
Et introduksjonskurs som har sikkerhet som et sentralt tema bør gjennomføres av alle ansatte så snart som mulig etter ansettelse. Kurset bør beskrive virksomhetens rutiner og retningslinjer innenfor sikkerhet. Relevante temaer i opplæringen kan være:

- Introduksjon av virksomheten og dens betydning for kritisk infrastruktur
- Kraftforsyningens verdi i et samfunnssikkerhetsperspektiv
- Risikoforståelse
- Trusselbildet, herunder trusselaktørers mål og metoder
- Innsidetrusselen, herunder fenomenbeskrivelse og kategorier
- Hva er kraftsensitiv informasjon, merking av informasjon og informasjonshåndtering
- Taushetserklæring og taushetsplikten – hva den gjelder, samt varighet. Gjeldende også etter at man har avsluttet arbeidsforholdet
- Digital sikkerhet og oppførsel på nett
- Reisesikkerhet. Gi informasjon og råd om situasjoner som kan oppstå på reise, hvordan dette kan forebygges og håndteres. Politiets sikkerhetstjeneste og Politidirektoratet har utgitt en håndbok som kan benyttes [xvi].

Etablere og gjennomføre opplæringsprogram for ledere

I tillegg til et introduksjonskurs for alle ansatte bør det utvikles et ledelsesprogram med opplæring i personellsikkerhet. Forventninger og retningslinjer til sikkerhet bør også inngå som del av lederhåndboken. For ledere kan et program for eksempel bygges opp med følgende innhold:

- Sikkerhetskultur – hva er det, hva betyr det for sikkerhet og hvordan du som leder er helt sentral i utviklingen av en god sikkerhetskultur
- Hvorfor og hvordan ha sikkerhet som et tema på ledermøter og i andre fora
- Hvordan snakke med dine ansatte om sikkerhet i medarbeidersamtalen
- Hvordan og når man bør tilby sårbarhetssamtaler
- Hvordan skape et åpent og tillitsfullt miljø der ansatte tør å komme til deg med sine bekymringer og ev. sikkerhetsutfordringer
- Leders rolle i å fremme bevissthet om sikkerhet blant ansatte

Gjennomføre kontinuerlige opplærings- og bevisstgjøringsaktiviteter

Sikkerhetstenkning er «ferskvare» og bevisstgjøring krever kontinuerlig arbeid. Som del av den daglige sikkerhetsmessige styringen bør det derfor utarbeides jevnlige bevisstgjøringskampanjer og obligatorisk opplæring. Aktivitetene kan gjennomføres som interne/eksterne foredrag, digitale kurs, temadager, faglunsjer m.m. og tilpasses virksomhetens behov og ønsker fra ansatte. Temaene kan inkludere for eksempel:

- Utfordringer man ser i virksomheten som påvirker sikkerhetskulturen (manglende bruk av adgangskort, mangelfull kunnskap om informasjonshåndtering, ulåste PCer og dører e.l.)
- Relevante temaer eller trender som dukker opp i nyhetsbildet og som er relevant for kraftforsyningen
- Temaer som ansatte ønsker å lære mer om
- Hvordan melde fra om mistenkelige hendelser (interne rutiner)
- Temaer fra introduksjonskurset kan med fordel følges opp i disse aktivitetene.

Etablere varslingssystem for ansatte knyttet til personellsikkerhet

En viktig del av det å avdekke innsidevirksomhet er et varslingssystem eller rapporteringssystem som gjelder bekymringer knyttet til innsidevirksomhet.

Det er viktig at hver virksomhet i kraftforsyningen har etablert et varslingssystem som er kjent for alle i virksomheten. Ansatte må gjøres kjent hvem de varsler til, hvordan og hva innholdet skal omfatte. Opplæring og kunnskap om menneskelige sårbarheter kan gi ansatte grunnlag for å vurdere når det kan og bør varsles.

Virksomheten velger selv om det varsles til en intern rolle eller til en ekstern uavhengig tredjepart. Dette varslingssystemet kommer i tillegg til avvikssystemer som virksomheter har som tar for seg andre type avvik og hendelser. Bekymringer knyttet til innsidevirksomhet bør ivaretas på en egnet måte, der beskyttelse av personopplysninger i henhold til regelverket står sentralt.[xvii]

Videreutvikle medarbeidersamtalen

Medarbeidersamtalen er en god anledning til å ta opp forskjellige emner også utover de mer vanlige temaene som jobbtilfredshet, utvikling, måloppnåelse m.m. Eksempler på dette kan være IT-sikkerhet, fysisk sikkerhet, personellsikkerhet og påminnelse om taushetserklæringen. Ved å skape en bevisstgjøring og alminneliggjøring rundt temaet personellsikkerhet, vil dette kunne bidra til å redusere opplevelsen av stigmatisering og mistenkeliggjøring.

Leder bør i tillegg minne ansatte om varslingssystemet som skal ivareta bekymringer knyttet til personellsikkerhet, dersom noe skulle oppstå på et senere tidspunkt. Det bør også opplyses om at andre i organisasjonen kan kontaktes (som f.eks. sikkerhetsleder) i tilfeller hvor den ansatte ikke er komfortabel med å diskutere dette med sin nærmeste leder.

Det å fange opp misfornøyde ansatte er et viktig arbeid, spesielt i endringsprosesser med oppkjøp, sammenslåinger eller andre organisasjonsendringer. I slike perioder med endringer kan det vurderes om det skal gjennomføres hyppigere samtaler med ansatte for å fange opp slike forhold.

Gjennomføre sårbarhetssamtaler

En sårbarhetssamtale er en frivillig samtale som bør tilbys ansatte med sårbarheter som kan gjøre dem mer attraktive for trusselaktører eller som på andre måter gjør dem sårbare i et personellsikkerhetsmessig perspektiv[xviii].

Sårbarhetssamtaler bør være regulert gjennom en prosedyre som beskriver formål, omfang, ansvar, når det bør gjennomføres, innhold, rammer, målgruppe, deltagere og dokumentasjon.

Det bør utarbeides et skjema for når samtaler har funnet sted og hvem som deltok. Det skal ikke skrives referat fra samtalen.

Når slike samtaler finner sted er det viktig å presisere at man ikke har noen mistanke til at vedkommende har gjort noe galt. Målet med samtalen er at den ansatte skal kjenne seg trygg i egen organisasjon, og at den ansatte forstår at man kan ta kontakt med personalleder eller sikkerhetsleder dersom vedkommende å ta opp forhold tilknyttet egne sårbarheter. Det er viktig at den ansatte forstår at informasjon om sårbarheter kan deles uten at dette får konsekvenser for arbeidsforholdet.

Eksempler på sårbarheter er når gjelde ansatte:

- har opplevd mistenkelige henvendelser
- har blitt forsøkt rekruttert
- har blitt utsatt for press mot seg selv eller personer i nære relasjoner
- frykter eller har økt risiko for press fra andre stater fordi man besitter kunnskap eller informasjon som kan gjøre en sårbar eller interessant
- har økonomiske problemer som kan gjøre en ekstra utsatt for press
- har samlivsproblemer som kan resulterer i at man er ekstra sårbar for press
- har utfordringer i omgang med rusmidler

Generelle råd for gjennomføring av samtalen:

- Samtalen må gjennomføres på egnet sted, slik at andre ikke kan overhøre/lytte til samtalen.
- Siden samtale om sårbarheter kan være sensitivt og medføre risiko for den ansatte, bør telefon, PC mv. i rommet settes på flymodus eller legges på annet sted før samtalen gjennomføres.
- Samtalen kan innledes med å forklare at virksomheten gjennomfører slike samtaler fordi den forvalter kraftsensitiv informasjon, og at kritiske objekter og infrastruktur kan være av interesse for andre. Dersom dette allerede er omtalt i rekrutteringsfasen, kan det bidra til at samtalen ikke oppleves som en mistenkeliggjøring eller stigmatisering.
- Diskuter forhold ved stillingen til den ansatte som kan gjøre vedkommende, eller informasjonen vedkommende sitter på, interessant for andre.
- Det er viktig at det ikke stilles spørsmål som kan gi inntrykk av at man har noen mistanke til en ansatt, men gi gjerne den ansatte mulighet til å fortelle om egne erfaringer.
- Åpne spørsmål innbyr til refleksjon og utdypende svar. Unngå spørreordet hvorfor, da dette kan sette den ansatte i forsvarsposisjon og gjøre samtalen videre mer lukket.
- Dersom leder er usikker på risikoen tilknyttet informasjon som mottas, kan man si at man ønsker å rådføre deg med sikkerhetsleder.
- Avslutt med å takke for at den ansatte deltok i samtalen, og presiser igjen at virksomheten gjør dette for å hjelpe ansatte som kan ha blitt, eller kan bli, utsatt for press. Gjenta gjerne at dette er samtaler som gjennomføres

rutinemessig med ansatte med tilknytning til høyrisikoland dersom det er aktuelt, eller ansatte som av andre grunner kan ha økt risiko for å bli utsatt for press.

Gjennomgå tilgangsstyringen regelmessig

I virksomheter vil det til enhver tid være forskjellige behov for både fysiske og digitale tilganger blant ansatte. Tilgangsstyring er i den sammenheng viktig for å hindre at uautoriserte får tilgang til informasjon, systemer og anlegg de ikke skal ha tilgang til[xix]. I tillegg vil unødvendige tilganger kunne gjøre ansatte mer sårbare både for bevisst og ubevisst innsidevirksomhet.

For å arbeide strukturert med tilgangsstyring er det nødvendig å kartlegge brukere og tilgangsbehov. I styringssystemet for sikkerhet bør det utarbeides interne rutiner med prosessbeskrivelser over hvem som skal ha tilgang til hva, hvordan tilganger gis og hvordan tilganger avsluttes. I disse rutinene bør det beskrives hvordan tilgangene gjennomgås regelmessig, samt når ansatte skifter stillinger internt.

Videre kan tilgangsstyring inkluderes som tema i opplæringen for ansatte for å informere om betydningen av riktig tilgangsstyring og beste praksis eller ønsket bruk av interne systemer og informasjon.

Inkludere innsidevirksomhet i beredskapsplanverk

I virksomhetens beredskapsplaner bør det inkluderes prosedyrer for varsling og håndtering av hendelser som er knyttet til innsiderisiko. I beredskapsøvelsene som virksomheten gjennomfører er det relevant å øve på scenarioer som innebærer innsidevirksomhet.

I utgangspunktet bør relevante hendelser for virksomheten tilpasses egne beredskapsplanverk og metoder for håndtering. I hendelser som er tilknyttet innsidevirksomhet kan det derimot være at varslingen og håndteringen bør være annerledes enn for andre type hendelser. I en situasjon med innsidevirksomhet vil det kunne være viktig å involvere færrest mulig da det er personsensitivt og har potensielt mange usikkerhetsmomenter. Det er viktig å tenke over hvordan informasjonen dokumenteres/loggføres, samt vurdere hvorvidt man bør varsle PST med tanke på bistand i videre håndtering.

Skadebegrensende tiltak bør være i fokus i planverket og hendelseshåndteringen. I håndteringsfasen vil det være viktig å tenke på hvordan situasjonen kan utvikle seg slik at man er proaktiv og fremtidsrettet.[xx]

Under er en punktvis liste som kan videreutvikles og tilpasses virksomheten, og som kan gi en retning på håndtering i en innledende fase:

- Varsle CEO/administrerende direktør og sikkerhetsleder eller annen relevant funksjon. Hvem som skal varsles vil kunne avhenge av situasjon og kjennskap til detaljer.
- Vurder hvem som skal involveres internt i hendelseshåndteringen i en innledende fase
- Vurder hvordan dette skal dokumenteres og sørg for en tilpasset dokumentering som er lukket/tilgangsstyrt
- Varsle PST ved behov for bistand til videre håndtering og kommunikasjon

5.2.1 Oppsummerte anbefalte tiltak

Anbefalte tiltak for daglig sikkerhetsmessig styring	
1	Gjennomføre bakgrunnssjekk av ansatte ved endring av stilling internt i virksomheten
2	Etablere og gjennomføre opplærings- og bevisstgjøringsprogram for alle ansatte
3	Etablere varslingssystem knyttet til personellsikkerhet
4	Videreutvikle medarbeidersamtalen - gjør sikkerhet og ivaretakelse til en naturlig del av samtalen
5	Gjennomføre sårbarhetssamtaler
6	Sørge for gode interne rutiner og oppfølging av fysiske og digitale tilganger
7	Inkludere innsidevirksomhet i beredskapsplanverket og øvelser

5.3 DEL 3 - Avslutning av ansettelsesforholdet

Rutiner knyttet til avslutning av et arbeidsforhold bør være en integrert del av virksomhetens systematiske arbeid med personellsikkerhet.

Ved avslutningen av ansettelsesforhold bør virksomheten gjennomføre konkrete tiltak for å begrense at utstyr og sensitiv informasjon kommer på avveie og utgjør en sikkerhetsrisiko. Dette gjelder alt fra adgangskort og PC til nøkler og dokumenter.

Når personer slutter i sine stillinger er det hensiktsmessig å kjenne årsaken til at vedkommende slutter. Var det en frivillig oppsigelse, en kontrakt som ikke ble fornyet eller en avskjedigelse av andre årsaker. Noen årsaker kan kreve ekstra oppmerksomhet i oppsigelsestiden. Opplevd urettmessig behandling, frustrasjon med mer kan i verste fall få negative konsekvenser for virksomheten. Dersom en ansatt slutter mot sin vilje, er det spesielt viktig med en avslutningssamtale. I tillegg er det behov for å gjennomgå tilgangene til vedkommende. Kanskje skal det i an avsluttende fase vurderes å begrense tilgangene til systemer eller anlegg.

Sørg for at fysiske og digitale tilganger til systemer og anlegg deaktiveres senest siste arbeidsdag. Det kan også være relevant å be om oversikt over eksterne, tjenestemessige tilganger vedkommende har, slik at disse kan deaktiveres (for eksempel i Brønnøysundregistrene eller NAV).

En god håndtering av ansatte i avslutningsfasen kan betraktelig redusere risikoen for uønskede hendelser i oppsigelsestiden og etter at arbeidsforholdet er avsluttet.

Vurder om det er samarbeidspartnere eller kontraktører som bør informeres om at ansettelsesforholdet opphører.

En avslutningssamtale bør gjennomføres som et fysisk møte og av andre enn nærmeste leder. Avslutningssamtalen bør ha sikkerhet som et eget tema. Samtalen bør avklare om det er behov for oppfølging etter endt arbeidsforhold. I tillegg er det helt sentralt at den ansatte minnes om taushetserklæringen vedkommende signerte ved oppstart. Kanskje er det lenge siden vedkommende signerte denne avtalen, eller kanskje er det ikke alltid at en har tydelig for seg at informasjonen en beskytter, også skal beskyttes etter endt arbeidsforhold.

5.3.1 Oppsummerte anbefalte tiltak

Anbefalte tiltak i avslutningsfasen	
1	Sørge for innlevering av utstyr og dokumenter
2	Gjennomgå og deaktiver tilganger og brukerkontoer
3	Informere kunder og samarbeidspartnere om at vedkommende slutter og sørg for at de har kontaktdetaljer til ny kontaktperson i selskapet
4	Gjennomføre avslutningssamtale – minn spesielt om forpliktelser vedrørende taushetserklæringer

6 Bruk av underleverandører

Ansatte hos underleverandører inklusive konsulenter, er i prinsippet underlagt samme krav og retningslinjer som egne ansatte.[xxi.] Med andre ord skal man stille de samme kravene og forvente det samme av underleverandører og andre eksterne virksomheter.[xxii]

I forberedende faser, for eksempel anbudsutlysning, bør det inkluderes sikkerhetskrav som en del av anbudsrunden når man velger underleverandører. Dette bidrar til å vise at sikkerhet blir tatt på alvor i virksomheten. Dette kan tiltrekke seg leverandører som tar sikkerhet på alvor, samt virke avskrekkende på leverandører som har uærlige hensikter. Utarbeidelse av sikkerhetskrav til underleverandører er viktig for å sikre at verdiene til virksomheten blir tilstrekkelig beskyttet.

Følgende tiltak kan være hensiktsmessige for å definere sikkerhetskrav samt for å redusere risikoen ved tjenesteutsetting og til å følge opp underleverandører:

Gjennomfør risikovurdering

Før man skal tjenesteutsette deler av virksomheten anbefales det å vurdere risikoer som er knyttet til tjenestene eller områdene som skal leveres av en konsulent eller underleverandør. En slik risikovurdering er viktig for å kartlegge hvilke områder man kan iverksette tiltak og hvor det bør rettes ekstra oppmerksomhet når det kommer til å definere sikkerhetskrav i kontrakten med leverandør.[xxiii]

Undersøk virksomhet og personell som skal inn

Før man inngår kontrakt om en tjenesteutsetting, bør man gjennomføre vurderinger angående sikkerhet. I den forbindelse bør virksomhetens eierskap, struktur og historikk undersøkes. Prosjektets art, og i hvilken grad innleid personell får tilgang til kraftsensitiv informasjon, vil ha betydning for hvor grundig en slik selskapsgjennomgang bør være. For tjenesteutsetting til virksomheter fra land det knytter seg større usikkerhet til, bør det gjennomføres en systematisk gjennomgang av virksomheten - "due diligence".

Kontraktsmessige sikkerhetskrav

Kontraktene med underleverandørene bør inneholde tydelige sikkerhetskrav. Definer krav til personellsikkerhet, kommunikasjon, periodiske inspeksjoner/revisjoner og frekvens samt innhold til rapportering, og henvis til virksomhetens styringssystem for sikkerhet med relevante dokumenter som både gjelder fast ansatte og annet eksternt personell.

Vurder å inkludere bestemmelser i kontraktene som klargjør ansvar og eventuell økonomisk kompensasjon i tilfelle brudd på sikkerhetsforpliktelser.

I de tilfeller der enkeltpersoner ikke kan signere taushetserklæringer på vegne av virksomheten er det ekstra viktig hvilke krav som stilles i kontrakt og at man vektlegger opplæring av underleverandørene.

Tydelig definerte roller og tilganger

Sørg for klarhet i hvilke oppgaver underleverandørene skal utføre og begrens tilganger til å gjelde det som er nødvendig for å utføre arbeidsoppgavene. Tilganger som gis utover det som er nødvendig øker potensialet for innsiderisiko.

Opplæring og bevissthet

På lik linje med internt ansatte bør det tilbys opplæring innen sikkerhet og innsiderisiko for underleverandører, konsulenter og andre eksterne. I tillegg bør kontrakten gjennomgås i detalj for å sikre forståelse av sikkerhetskrav.[xxiv] Som tidligere omtalt i 5.2 av denne veilederen, vil økt sikkerhetsbevissthet kunne bidra til å redusere risikoen for uaktsom eller uetisk atferd.

Oppfølging og periodiske inspeksjoner/revisjoner:

Etabler rutiner for periodisk oppfølging av underleverandørene for å undersøke om kontrakten og de interne sikkerhetsrutinene til virksomheten overholdes over tid. En tydelig beskrivelse av de periodiske inspeksjonene må avtales før kontrakten signeres.[xxv]

Opphør (off-boarding) og avslutningssamtale

Ved opphør av kontrakt med underleverandører, bør tiltakene for avslutning av ansettelsesforhold i kapittel 5.3 gjennomføres så langt det er mulig.

6.1.1 Oppsummerte anbefalte tiltak

	Tiltak i forbindelse med bruk av underleverandører
1	Beskriv sikkerhetskrav i anbudsprosess og senere i avtaler med underleverandører
2	Gjennomfør en risikovurdering av det som skal tjenesteutsettes
3	Vurder virksomhet og personell som skal utføre arbeidet
4	Sørg for korrekt tilgangsstyring for underleverandør
5	Gjennomfør opplæring med valgt leverandør og gjennomgå sikkerhetskrav i avtalene
6	Følg opp leverandør gjennom prosjektet
7	Gjennomfør avslutningsprosedyrer på lik linje som ved egne ansatte

7 Det juridiske handlingsrommet

Ulike lovverk regulerer det juridiske handlingsrommet for kraftforsyningen i spørsmål knyttet til personellsikkerhet. I mange tilfeller vil det være ulike krav, hensyn og interesser som skal ivaretas, og det er ikke alltid åpenbart hvordan dette skal vektes når flere regelverk kommer til anvendelse.

Det er derfor viktig å huske på at flere lovverk åpner opp for at det kan og bør gjøres individuelle og konkrete vurderinger. Dette forutsetter god juridisk kompetanse om sentrale lovverk, enten internt eller ved ekstern bistand. Det er særlig viktig å gjøre seg kjent med unntaksbestemmelser for å kunne utforske mulighetene som lovverket gir.

Likestillings- og diskrimineringsloven (ldl) åpner eksempelvis for at ikke all forskjells-behandling er diskriminering. Det kan foreligge legitime grunner til å behandle personer forskjellig. Forskjellsbehandling regnes ikke som diskriminering når den har et saklig formål, er nødvendig for å oppnå formålet og det er et rimelig forhold mellom det man ønsker å oppnå og hvor inngripende forskjellsbehandlingen er for den/de som stilles dårligere.

Her er det verdt å merke seg at utdanningsland, tidligere arbeidsopphold, landopphold, aksjer og eiendom er forhold som ikke omfattes av etnisitetsbegrepet. Forskjellsbehandling på grunn av statsborgerskap er i utgangspunktet heller ikke vernet av diskrimineringsloven om etnisitet, jf. oppramsingen i ldl § 6 første og andre ledd. Det fremgår imidlertid av forarbeidene til tidligere diskrimineringslov av 2005, som i hovedsak er videreført, at forskjellbehandling på grunn av statsborgerskap *kan* rammes av forbudet mot indirekte diskriminering på grunn av etnisitet.

Dette eksemplifiserer igjen behovet for å gjøre konkrete og individuelle vurderinger, med vekt på saklig formål, nødvendighet og forholdsmessighet, for å redegjøre for hvorvidt indirekte forskjellbehandling vil være lovlig eller ikke, jf. ldl § 9.

Avslutningsvis er det nødvendig å understreke at i alle saker som omhandler ansatte og personellsikkerhet er det viktig å inkludere fagforeninger, HMS og verneombud i tidlige faser. Dersom man har etablert et sikkerhetsteam, vil dette også være en viktig ressurs som kan ivareta en helhetlig tilnærming til komplekse problemstillinger.

7.1 Sentrale lovverk

- Kraftberedskapsforskriften
  - https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157
- Sikkerhetsloven
  - https://lovdata.no/dokument/NL/lov/2018-06-01-24
- Energiloven
  - https://lovdata.no/dokument/NL/lov/1990-06-29-50
- Virksomhetssikkerhetsforskriften
  - https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053
- Arbeidsmiljøloven
  - https://lovdata.no/dokument/NL/lov/2005-06-17-62
- Likestillings- og diskrimineringsloven
  - https://lovdata.no/dokument/NL/lov/2017-06-16-51

- Personopplysningsloven
    - https://lovdata.no/dokument/NL/lov/2018-06-15-38

Vedlegg 1

Kilder som kan være nyttige, og relevante problemstillinger som bør vurderes i forbindelse med tjenesteutsetting

- Har landet høyere risiko knyttet til kreditt- og betalingsrisiko etter OECDs risikoklassifisering - https://www.eksfin.no/no/landrisiko/
    - Er det god forretningsstabilitet i landet? - F.eks. hvor stor grad privat næringsliv i landet har råderett uten statlig innblanding og statlige føringer.
- Er det høyere korrupsjon i landet? - https://www.transparency.org/en/cpi
- Er det politisk stabilitet i landet? - https://www.theglobaleconomy.com/economies/
- Vurderes det at lover og regler i landet overholdes og at man har tillit til disse? "F.eks. overholdelse av inngåtte kontrakter, tillit til politiet og domstolene, slik at «Rule of law» generelt følges. - https://worldjusticeproject.org/rule-of-law-index/"
- Vurderes landet å være fredelig med god samfunnssikkerhet, og ha et lavt nasjonalt og internasjonale konfliktnivå? - https://www.visionofhumanity.org/maps/#/
- Er landet vurdert til å være et høyrisikoland av The Financial Action Task Force (FATF)? - https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html
- Har Norge et økonomisk eller internasjonalt samarbeid med landet? F.eks. EU. - https://european-union.europa.eu/principles-countries-history/country-profiles_en
- Har Norge et sikkerhetsmessig samarbeid med landet? F.eks. via NATO - https://www.nato.int/cps/en/natohq/nato_countries.htm
- Ved overføring av personopplysninger til 3-parter, er landet vurdert til å ha tilstrekkelig beskyttelse? - https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/
- Vurderes IT og IT-sikkerhet i landet å være modent? "F.eks. er IKT-infrastruktur godt utbygget og utbygde nasjonale IKT-tjenester, kompetanse på IT-sikkerhet, etablert CERT-struktur og internasjonalt samarbeid. - https://ncsi.ega.ee/

8 Referanser

[i] Nasjonal Sikkerhetsmyndighet (NSM). 2023. https://nsm.no/fagomrader/sikkerhetsstyring/hva-er-sikkerhetsstyring/

[ii] Forsvarsbygg. 2022. Sikringshåndboka

[iii] Nasjonal Sikkerhetsmyndighet (NSM). 2023. Grunnprinsipper for personellsikkerhet https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/

[iv] Forsvarsbygg. 2022. Sikringshåndboka

[v] Reason, J. (1997). Managing the Risks of Organizational Accidents. Ashgate Publishing Limited: Surrey.

[vi] Martin, 2019. Gjengitt i FFI. 2023. Hva vet vi om innsiderisiko. https://www.ffi.no/publikasjoner/arkiv/hva-vet-vi-om-innsiderisiko

[vii] Nasjonal Sikkerhetsmyndighet (NSM). 2023. Risiko. https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

[viii] Nasjonal Sikkerhetsmyndighet (NSM). 2020. Landvurdering ved tjenesteutsetting av IKT-tjenester https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/landvurdering-ved-tjenesteutsetting-av-ikt-tjenester

[ix] Nasjonal Sikkerhetsmyndighet (NSM). 2020. Sikkerhetsfaglige anbefalinger ved tjenesteutsetting https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/gode-risikovurderinger-for-a-kunne-ta-riktig-beslutning/

[x] Politiets Sikkerhetstjenestes (PST) Nasjonale trusselvurderinger 2021/2023. https://www.pst.no/

[xi] Næringslivets Sikkerhetsråd (NSR). 2021. Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO). https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino

[xii] The NATO Cooperative Cyber Defence Centre of Excellence (CDCOE). 2018. Insider threat study. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

[xiii] National Protective Security Authority (NPSA – tidligere CPNI). 2023. CPNI insider data collection study

[xiv] Australian Government. 2023. A guide for Australian Government – countering the insider threat https://www.ag.gov.au/integrity/publications/countering-insider-threat-guide-australian-government

[xv] Næringslivets Sikkerhetsråd (NSR). 2017. Sikkerhet ved ansettelsesforhold. https://www.nsr-org.no/uploads/documents/Publikasjoner/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

[xvi]Sikker reise. Politiets Sikkerhetstjenest (PST)/Politidirektoratet (POD)2017. https://www.pst.no/globalassets/eldre/sikker_reise_2017_nettsiden.pdf

[xvii] Datatilsynet. 2022. Personvern på arbeidsplassen. https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/varsling/?print=true

[xviii] Nasjonal Sikkerhetsmyndighet (NSM).2020. Grunnprinsipper for personellsikkerhet: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/beskytte/legg-til-rette-for-sarbarhetsoppfolging/

[xix] Nasjonal Sikkerhetsmyndighet (NSM). 2020. Grunnprinsipper for IKT sikkerhet. https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

[xx] Lunde, Ivar Konrad. 2019. Praktisk krise og beredskapsledelse.

[xxi] Næringslivets Sikkerhetsråd (NSR). 2017. Sikkerhet ved ansettelsesforhold. https://www.nsr-org.no/uploads/documents/Publikasjoner/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

[xxii] Nasjonal Sikkerhetsmyndighet (NSM). 2021. Veileder i anskaffelser etter sikkerhetsloven. https://nsm.no/getfile.php/136607-1698049737/NSM/Filer/Dokumenter/Veiledere/Veileder%20i%20anskaffelser%20etter%20sikkerhetsloven.pdf

[xxiii] Næringslivets Sikkerhetsråd (NSR). 2017. Sikkerhet ved ansettelsesforhold. https://www.nsr-org.no/uploads/documents/Publikasjoner/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

[xxiv] National Protective Security Authority (NPSA). 2023. Personnel Security Guidance - A Good Practice Guide for Employers file:///C:/Users/pki561/Downloads/npsa-persec-contractors-good-practice-guide.pdf

[xxv] National Protective Security Authority (NPSA). 2023. Personnel Security Guidance - A Good Practice Guide for Employers file:///C:/Users/pki561/Downloads/npsa-persec-contractors-good-practice-guide.pdf

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95