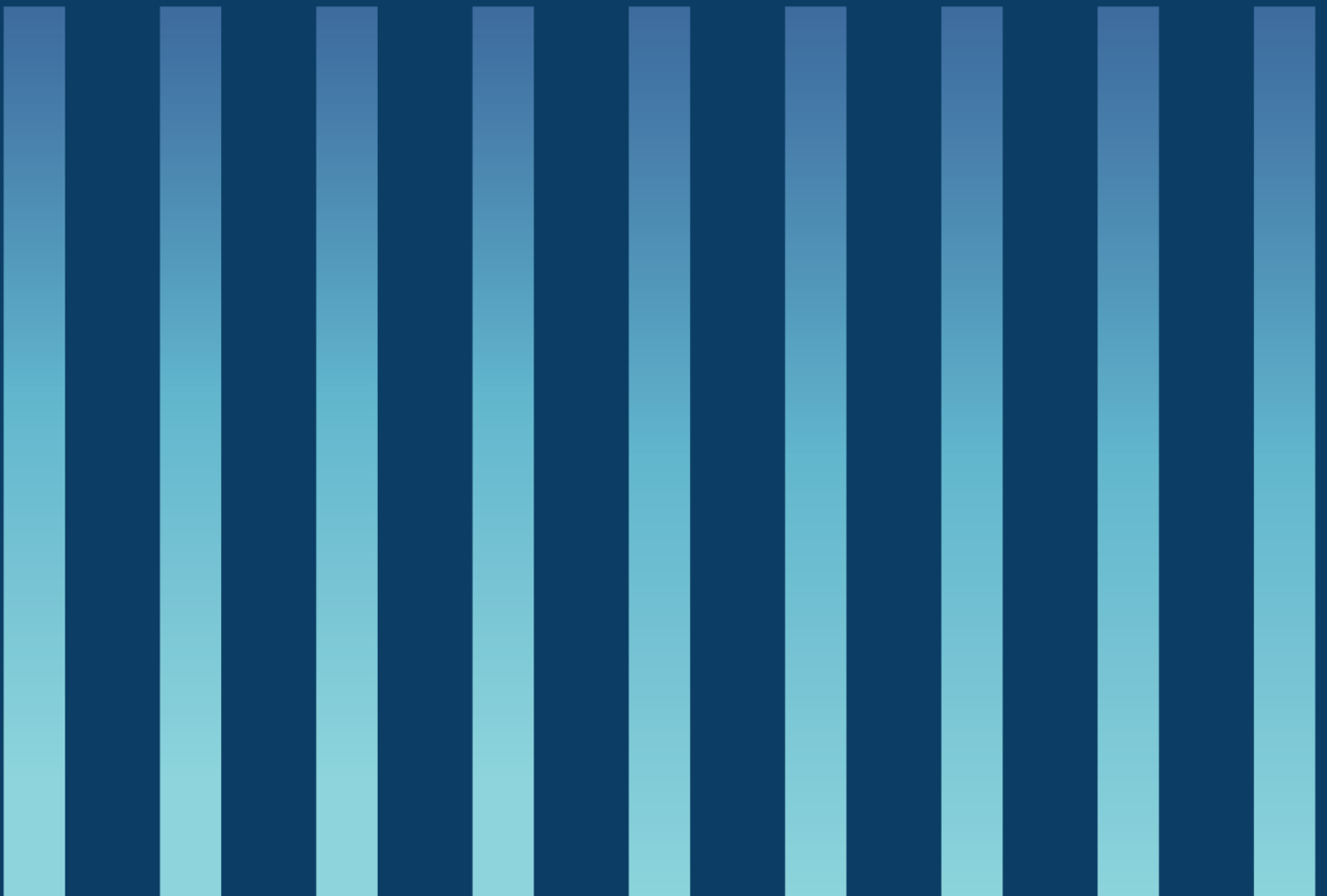




Grunnprinsipper for personellsikkerhet

Versjon: [Versjon]



INNHOILDSFORTEGNELSE

Introduksjon	4
1. Identifisere og kartlegge	6
1.1. Foreta stillings- og oppdragsspesifikke risikovurderinger.....	6
1.2. Ha en sikkerhetsbasert tilnærming til rekruttering.....	6
2. Beskytte	8
2.1. Integrer personellsikkerhet i sikkerhetsstyringen	8
2.2. Reduser risiko under ansettelsesforhold.....	8
2.3. Innfør et effektiv rapporteringssystem.....	9
2.4. Legg til rette for sårbarhetsoppfølging	9
2.5. Etabler rutiner for hendelseshåndtering.....	10
3. Opprettholde og oppdage	11
3.1. Skape en god sikkerhetskultur.....	11
3.2. Ivareta medarbeidere gjennom tilpasset oppfølging	11
3.3. Følg opp medarbeidere med identifiserte sårbarheter.....	12
3.4. Avdekk nye personellsikkerhetsmessige sårbarheter	13
3.5. Avklar årsaken til endringer i medarbeidernes atferd	13
3.6. Ivareta sikkerheten ved avvikling av arbeidsforhold	14
4. Håndtere og gjenopprette	15
4.1. Håndter hendelser proporsjonalt.....	15
4.2. Begrens skadene så raskt og så mye som mulig	15
4.3. Ivareta medarbeiderne også under hendelseshåndtering	16
4.4. Evaluer hendelser og håndteringen av dem.....	16
4.5. Lær av erfaringer og implementer endringer	17

Identifisere og kartlegge	Beskytte	Opprettholde og oppdage	Håndtere og gjenopprette
Foreta stillings- og oppdragsspesifikke risikovurderinger	Integrer personellsikkerhet i sikkerhetsstyringen	Skap en god sikkerhetskultur	Håndter hendelser proporsjonalt
Ha en sikkerhetsbasert tilnærming til rekruttering	Reduser risiko under ansettelsesforhold	Ivareta medarbeiderne gjennom tilpasset oppfølging	Begrens konsekvensene så raskt og så mye som mulig
	Innfør et effektivt rapporteringssystem	Følg opp medarbeidere med identifiserte sårbarheter	Ivareta medarbeiderne også under hendelseshåndtering
	Legg til rette for sårbarhetsoppfølging	Avdekk nye personellsikkerhetsmessige sårbarheter	Evaluer hendelser og håndteringen av dem
	Etabler rutiner for hendelseshåndtering	Avklar årsaken til endringer i medarbeidernes atferd	Lær av erfaringer og implementer endringer
		Ivareta sikkerheten ved avvikling av arbeidsforhold	

Introduksjon

Samfunnsmessige endringer fører til at stadig flere personer får tilgang til virksomheters verdier. En rask teknologisk utvikling, økende IKT-avhengighet og et stadig større digitaliseringsbehov gjør at virksomheter trenger flere personer til å forvalte verdiene. Samtidig bidrar nye digitale arenaer og plattformen til at trusselaktørenes mulighetsrom øker. Både statlige og ikke-statlige trusselaktører fortsetter å bruke metoder for å kartlegge og dra nytte av personer på innsiden av virksomheter. Hovedårsaken til dette er at personer på innsiden har en direkte eller indirekte tilgang til verdiene, og at personer i større eller mindre grad har sårbarheter som en trusselaktør kan forsøke å utnytte.

Tiltak innenfor personellsikkerhet utgjør derfor en viktig del av virksomheters arbeid for å beskytte verdiene sine. Uønsket påvirkning kan medføre en rekke negative konsekvenser for aktører som eier, forvalter eller drar nytte av verdiene. Noen virksomheter forvalter verdier av betydning for nasjonale sikkerhetsinteresser, mens andre forvalter verdier av stor betydning for samfunnet eller dem selv. En god forståelse av eget risikobilde gjør at virksomheter kan identifisere personellsikkerhetsmessige tiltak som begrenser trusselaktørenes mulighetsrom og som øker virksomhetens egen sikkerhetsmessige robusthet.

Formålet med personellsikkerhet

For å ivareta personellsikkerheten er det avgjørende at virksomheter implementerer tiltak som reduserer risikoen for innsiddevirksomhet. Innsiddevirksomhet defineres som tilfeller der en nåværende eller tidligere medarbeider¹ misbruker sin tilgang eller kunnskap for å utføre handlinger som påfører virksomheten skade eller tap.² Det kan være flere grunner til at en medarbeider begår innsiddevirksomhet. En bevisst innsider kan være selvmotivert eller påvirket av en ekstern aktør, hvorimot en ubevisst innsider begår handlingene uten at det er intensjonen. Dette er perspektiver som bør inngå i virksomhetenes arbeid med å forebygge, avdekke og håndtere innsiddevirksomhet. Tiltak som tar for seg det menneskelige aspektet ved dette arbeidet, er tiltak som hører innunder personellsikkerhet.

Gjennom en god sikkerhetskultur og bevisstgjørende tiltak kan virksomheter opprettholde og styrke personellsikkerheten. Enhver medarbeider er med på å forme virksomhetens kultur, verdier og holdninger. Hvordan medarbeidere forholder seg til sikkerhet, kan derfor ha en reell innvirkning på virksomhetens risikobilde. Rollen som medarbeider medfører blant annet et ansvar for å beskytte verdiene og melde fra om sikkerhetsstruende hendelser. Den enkelte virksomhet bør derfor sørge for å motivere sine medarbeidere, og innarbeide deres rolle og bidrag i det daglige sikkerhetsarbeidet. Formålet er å bygge opp medarbeiderne til å bli effektive barrierer mot trusler både utenfor og innenfor virksomheten.

Ledere har et overordnet ansvar for å påse at virksomheten har tilstrekkelig med kompetanse og ressurser til å ivareta en god personellsikkerhet. Det er ledernes ansvar å sikre at sikkerhetskulturen er sterk, at sårbarheter fanges opp, og at sikkerhetsrelaterte hendelser håndteres effektivt. For å gi virksomheter et utgangspunkt i arbeidet med personellsikkerhet, har Nasjonal sikkerhetsmyndighet (NSM) utarbeidet grunnprinsipper for personellsikkerhet.

Hva er NSMs grunnprinsipper for personellsikkerhet?

NSMs grunnprinsipper for personellsikkerhet presenterer et sett med anbefalte tiltak som forteller hva virksomheter bør gjøre for å skape et helhetlig system for personellsikkerhet. Grunnprinsippene beskriver **hva** virksomheten bør gjøre, **hvorfor** det bør gjøres, men i liten grad **hvordan** det bør

¹ Begrepet medarbeider inkluderer her faste, midlertidige og innleide medarbeidere.

² Les mer om dette i NSMs temarapport om innsiderisiko (2019).

gjøres. Valg av konkrete personellsikkerhetsmessige tiltak bør som alltid baseres på virksomhetens egne behov, muligheter, krav og begrensninger.

Grunnprinsippene for personellsikkerhet er tverrsektorielle, og skal være et utgangspunkt for alle virksomheter som ønsker å skape et helhetlig system for personellsikkerhet. Grunnprinsippene er ikke knyttet opp mot kravene i sikkerhetsloven eller andre regelverk. Virksomheten har et selvstendig ansvar for å vurdere om det er juridiske beskrankninger innenfor dens virkeområde som hindrer gjennomføringen av hvert enkelt tiltak. Virksomheter omfattet av sikkerhetsloven må sørge for at lovens krav til personellsikkerhet følges.

Grunnprinsippene for personellsikkerhet er strukturert etter fire kategorier. Dette er kategorier man vil kjenne igjen fra grunnprinsippene for sikkerhetsstyring, fysisk sikkerhet og IKT-sikkerhet:

1. Identifisere og kartlegge
2. Beskytte
3. Opprettholde og oppdage
4. Håndtere og gjenopprette

Under hver kategori finner man NSMs grunnprinsipper for personellsikkerhet. Deretter følger en beskrivelse av grunnprinsippet og en liste over anbefalte tiltak. Listene over tiltak er ikke uttømmende, men et sett med anbefalinger fra NSMs side.

Målgruppe

Målgruppen for grunnprinsippene er primært ledere og andre med ansvar for personellsikkerheten. For å sikre et akseptabelt sikkerhetsnivå er det avgjørende at ledelsen prioriterer og setter mål for hvordan virksomheten skal ivareta en god personellsikkerhet. Samtidig er NSM av den oppfatning at grunnprinsippene kan nyttiggjøres av andre aktører i virksomheten, eksempelvis mellomledere med oppfølgingsansvar og den enkelte medarbeider.

NSM har et mål om at grunnprinsippene for personellsikkerhet skal være et levende og tidsaktuelt produkt. Etter hvert som NSM får innspill fra brukere av produktet, kommer vi derfor til å oppdatere og videreutvikle grunnprinsippene.

Grunnprinsippene sett opp mot andre produkter

Det er viktig å legge merke til at grunnprinsippene for personellsikkerhet ikke er enkeltstående prinsipper, men må sees i sammenheng med virksomhetens sikkerhetsstyring og tiltak innenfor fysisk sikkerhet og IKT-sikkerhet. Virksomheter vil først kunne oppnå et akseptabelt sikkerhetsnivå når den har et sett med tiltak som både ivaretar det organisatoriske, teknologiske, fysiske og menneskelige aspektet. Uten et fullstendig perspektiv på sikkerhet vil det være vanskelig for virksomheter å sikre sine verdier i tilstrekkelig grad.

Grunnprinsippene for personellsikkerhet bør også sees i sammenheng med andre produkter som omhandler personellsikkerhet. Mer informasjon finnes eksempelvis i:

- NSMs temarapport om insidersisiko (2019)
- Sikkerhet ved ansettelsesforhold (PST, NSM, Politiet og Næringslivets sikkerhetsråd, 2017)
- Sektorspesifikke rapporter om håndtering av insidersisiko

1. Identifisere og kartlegge

Denne kategorien omhandler identifisering og kartlegging av risiko knyttet til stillinger, oppdrag og rekruttering av nye medarbeidere. Dette er vurderinger som krever kunnskap om virksomhetens verdier og ressurser. Kategorien har derfor en sterk forbindelse til virksomhetens sikkerhetsstyring, og må sees i sammenheng med virksomhetens overordnede verdi-, trussel- og sårbarhetsvurderinger. Disse danner grunnlaget for mer konkrete risikovurderinger knyttet til personellsikkerhet.

1.1. Foreta stillings- og oppdragsspesifikke risikovurderinger

Det anbefales at virksomheten vurderer risiko knyttet til konkrete stillinger og oppdrag. Dette innebærer at virksomheten kartlegger hvilke stillinger og/eller oppdrag som kan gi betydelig innblikk i sentrale deler av virksomheten, eller som av andre grunner kan gjøre medarbeidere særlig utsatt for rekrutteringsforsøk eller andre trusler.

Hvorfor er dette viktig: En samlet oversikt over utsatte stillinger og oppdrag gjør det lettere for virksomheten å identifisere tiltak som kan redusere risiko forbundet med disse.

Anbefalte tiltak:

- Utarbeid kriterier for å identifisere stillinger og oppdrag med forhøyet risiko.
- Vurder konsekvensene av innsidevirksomhet i de konkrete stillingene eller oppdragene.
- Avgjør om enkelte stillinger eller oppdrag skal medføre strengere krav til medarbeiderne og en mer omfattende bakgrunnsundersøkelse.
- Innfør individuelle og/eller gruppebaserte tiltak – for eksempel en tilpasset sikkerhetsopplæring for medarbeidere i utsatte stillinger.
- Sørg alltid for å foreta nye risikovurderinger ved endringer av relevans for personellsikkerheten – for eksempel endringer i trusselbildet.

1.2. Ha en sikkerhetsbasert tilnærming til rekruttering

Virksomheten bør ha en sikkerhetsbasert tilnærming til rekruttering og gjøre konkrete risikovurderinger i forkant av nyansettelser. Bakgrunnsundersøkelser, identifisering av sårbarheter og individuelle helhetsvurderinger er aktiviteter som kan redusere risiko forbundet med rekruttering.

Hvorfor er dette viktig: Gjennom en sikkerhetsbasert tilnærming til rekruttering kan virksomheten forhindre at personer som utgjør en risiko, plasseres slik at risikoen aktualiseres.

Anbefalte tiltak:

- Undersøk om aktuelle kandidater oppfyller virksomhetens krav til stillingen eller oppdraget, og foreta nødvendige bakgrunnsundersøkelser.
- Identifiser om aktuelle kandidater har personellsikkerhetsmessige sårbarheter som kan påvirke virksomhetens risikobilde.

- Vurder om det kan gjøres risikoreduserende tiltak overfor den enkelte og hvorvidt virksomheten kan akseptere en eventuell restrisiko.
- Påse at alle aktuelle kandidater har tilstrekkelig kompetanse om sikkerhet og har forstått sine plikter før de gis tilgang til virksomhetens verdier. Bekreft alltid personens identitet.
- Etabler et godt samarbeid med blant annet HR, arbeidstakerforeningene og juridisk avdeling for å ivareta sikkerheten og lovmessige krav ved rekruttering.
- Sikre at personer med hovedansvaret for å foreta bakgrunnsundersøkelser og individuelle risikovurderinger har tilstrekkelig kunnskap om hvordan slike prosesser skal gjennomføres.

2. Beskytte

Denne kategorien av grunnprinsipper beskriver hvordan virksomheten bør etablere rammer, systemer og rutiner innenfor personellsikkerhet som bidrar til å beskytte verdiene. Virksomheter som integrerer personellsikkerhet i sikkerhetsstyringen, reduserer risiko under ansettelsesforhold og innfører et effektivt rapporteringssystem, kan ivareta en god sikkerhetstilstand. I tillegg vil rutiner for henholdsvis sårbarhetsoppfølging og hendelsehåndtering skape forutsigbarhet når virksomheten skal følge opp endringer og hendelser av sikkerhetsmessig betydning.

2.1. Integrer personellsikkerhet i sikkerhetsstyringen

Personellsikkerhet bør inngå som en integrert del av virksomhetens helhetlige sikkerhetsstyring. Det menneskelige aspektet ved sikkerhet bør prioriteres av og forankres hos ledelsen. Dette krever en systematisk tilnærming som blant annet omfatter fagkompetanse, ressurser, rutiner og retningslinjer innen personellsikkerhet.

Hvorfor er dette viktig: Alle personellsikkerhetsmessige tiltak bør settes i system for å oppnå best mulig effekt og tilstrekkelig kontroll på sikkerhetstilstanden.

Anbefalte tiltak:

- Sørg for at personellsikkerhet prioriteres av virksomhetens ledelse.
- Tildel en eller flere ansatte oppgaver og det overordnede ansvaret for personellsikkerhet.
- Sikre at virksomheten har tilstrekkelig kompetanse og ressurser innenfor fagområdet.
- Skriftliggjør personellsikkerhetsmessige rutiner og retningslinjer.
- Evaluer menneskelige tiltak jevnlig, både på organisasjons-, gruppe- og individnivå.
- Mål ledere på gjennomføringen av personellsikkerhetsmessige prosedyrer/instrukser/rutiner etc. som en del av sikkerhetsstyringen. Mål både kvantitet og kvalitet.

Sikre at alle rutiner og retningslinjer gjennomføres i tråd med gjeldende lov- og regelverk om blant annet personvern (GDPR), arbeidsmiljø, likestilling, antidiskriminering, HMS og krav til offentlighet og privatlivets fred.

2.2. Reduser risiko under ansettelsesforhold

Som en følge av at medarbeidere gis tilgang til virksomhetens informasjon og verdier, vil de i et personellsikkerhetsmessig perspektiv alltid kunne utgjøre en risiko. Virksomheten bør derfor etablere rammer som reduserer risikoen for innsidevirksomhet, øker medarbeidernes sikkerhetsmessige bevissthet og gir økt kunnskap om sikkerhet.

Hvorfor er dette viktig: Manglende sikkerhetsmessige rutiner knyttet til ansettelsesforhold kan øke risikoen for bevisst og ubevisst innsidevirksomhet. Virksomheten bør derfor ha rutiner og prosesser som reduserer risikoen for at en potensiell innsider påfører den skade eller tap.

Anbefalte tiltak:

- Etabler tilgangs- og adgangsskilt som sikrer at medarbeidere kun gis tilganger som er nødvendige for å kunne utføre sine arbeidsoppgaver – «need to know»-prinsippet.
- Sørg for en jevnlig opprydding av tilgangsrettighetene.
- Hold obligatoriske introduksjons- og opplæringsprogram som beskriver virksomhetens rutiner og retningslinjer innenfor sikkerhet.
- Tydeliggjør virksomhetens forventninger til medarbeidernes handlemåter på arenaer som kan kreve høy sikkerhetsmessig bevissthet, for eksempel på utenlandsreiser, konferanser og sosiale medier.
- Påse at avvikling av arbeidsforhold igangsetter en obligatorisk prosess som ivaretar sikkerhetsmessige hensyn, blant annet avslutningssamtaler og sperring av tilganger.

2.3. Innfør et effektiv rapporteringssystem

Virksomheten bør etablere et system som fanger opp sikkerhetsrelaterte avvik. Dette gir mulighet til å iverksette tidsriktige og målrettede tiltak som begrenser potensielle skadefølger og forebygger nye avvik. Rapportering fra medarbeidere vil også kunne gi viktig informasjon som kan avdekke pågående eller tidligere innsiddevirksomhet.

Hvorfor er dette viktig: Et rapporteringssystem er viktig for å fange opp endringer i virksomhetens risikobilde og eventuelle andre forhold av betydning for sikkerhetstilstanden. Ved å følge opp avvik på en effektiv måte kan også virksomheten synliggjøre at rapporteringer tas på alvor.

Anbefalte tiltak:

- Legg til rette for at medarbeidere kan rapportere om sikkerhetsrelaterte forhold, for eksempel brudd på virksomhetens rutiner og retningslinjer.
- Sikre at alle medarbeidere vet hvilke forhold det bør rapporteres om og hvordan man rapporterer.
- Etabler rutiner for mottak, behandling og oppfølging av rapporteringer. Sørg for at det gis en rask tilbakemelding til medarbeidere som rapporterer og at personen ivaretas gjennom hele prosessen.
- Påse at rapporteringsrutinene utarbeides i samarbeid med ansatte og tillitsvalgte.
- Etabler kontaktpunkter med politi og eventuelt andre myndigheter.

2.4. Legg til rette for sårbarhetsoppfølging

Virksomheten bør legge til rette for oppfølging av medarbeidere med sårbarheter som kan gjøre dem til attraktive mål for en trusselaktør, eller som på andre måter gjør dem sårbare i et personellsikkerhetsmessig perspektiv. Virksomheten bør sørge for at alle medarbeidere er kjent med rutinene for sårbarhetsoppfølging. Tydelige og etablerte rutiner for hvordan virksomheten vil gå frem for å følge opp sårbarheter, skaper forutsigbarhet for medarbeiderne. Det vil også bidra til å synliggjøre virksomhetens egen støttefunksjon overfor medarbeidere med sårbarheter.

Hvorfor er dette viktig: Etablerte rutiner sikrer at alle medarbeidere har like forutsetninger for sårbarhetsoppfølging i virksomheten. Ettersom nye sårbarheter kan resultere i en økt risiko, er det likeledes viktig at virksomheten har rutiner for hvordan nye personellsikkerhetsmessige sårbarheter skal identifiseres og følges opp.

Anbefalte tiltak:

- Lag rutiner og retningslinjer som beskriver hvordan virksomheten skal følge opp personellsikkerhetsmessige sårbarheter og identifisere nye sårbarheter.
- Utarbeid egne rutiner for sårbarhetssamtaler. Rutinene bør som et minimum beskrive hensikten med sårbarhetssamtaler, når de skal avholdes, hvordan de skal avholdes og hvilke medarbeidere eller grupper av medarbeidere som er i målgruppen.
- Avklar hvem i virksomheten som skal ha ansvaret for sårbarhetssamtaler og hvilke andre ansatte som kan eller bør være til stede under samtalen, for eksempel ledere eller tillitsvalgte.
- Legg til rette for annen sårbarhetsreduserende oppfølging i virksomheten, blant annet tilpasset opplæring, avgrensning av arbeidsoppgaver og tilganger, og egenrapportering.
- Sørg for å gi tilstrekkelig opplæring til ledere og/eller andre med ansvar for å følge opp sårbarheter.

2.5. Etabler rutiner for hendelseshåndtering

Dette grunnprinsippet handler om å være forberedt på at innsideaktivitet og andre uønskede hendelser kan komme til å skje. Virksomheten bør ha en plan for hvordan den skal håndtere det menneskelige aspektet ved en potensiell hendelse.

Hvorfor er dette viktig: Utarbeidelse av egne rutiner er vesentlig for å være i stand til å håndtere uønskede og sikkerhetstruende hendelser, og dermed kunne gjenopprette og ivareta sikkerhetstilstanden i virksomheten.

Anbefalte tiltak:

- Utarbeid rutiner som beskriver når og hvordan hendelser skal undersøkes.
- Ha en tydelig rollefordeling som fastslår hvem i virksomheten som bistår med hva i håndteringsprosessen, for eksempel personer i IT, nærmeste leder, juridisk avdeling og HR.
- Sørg for at ansatte med utpekte roller gis nødvendig opplæring og trening.
- Utarbeid egne rutiner og retningslinjer for involvering av ekstern bistand. Beskriv hvilke hendelser som skal anmeldes til politiet og/eller varsles om til PST.
- Planlegg når og hvordan virksomheten skal formidle informasjon om sikkerhetsrelaterte hendelser til personer innenfor og utenfor virksomheten. Personer utenfor virksomheten kan for eksempel være representanter fra media eller andre eksterne aktører.
- Påse at kontinuitetsplanen (hvordan sikre videre drift) beskriver tiltak overfor personell.
- Sikre at alle sikkerhetsrelaterte hendelser loggføres og dokumenteres.

3. Opprettholde og oppdage

Denne kategorien handler om å opprettholde personellsikkerheten over tid. Et akseptabelt sikkerhetsnivå oppnås gjennom en prosess hvor virksomheten følger opp sine medarbeidere gjennom hele ansettelsesforholdet og ved avvikling av dette. Sentralt her er å følge opp eventuelle menneskelige sårbarheter, gi medarbeidere et oppdatert bilde av virksomhetens risikobilde, motivere dem til å ivareta virksomhetens retningslinjer og tilrettelegge for rapportering. Videre omfatter kategorien det å oppdage eller avdekke forhold av personellsikkerhetsmessig karakter som kan indikere innsiddevirksomhet eller annen sikkerhetsrelatert uønsket atferd hos medarbeiderne.

3.1. Skape en god sikkerhetskultur

En sikkerhetskultur kan defineres som et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet. Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, kan virksomheten skape en god sikkerhetskultur. Dette er i stor grad lederens ansvar, og fordrer at lederen går foran som et godt eksempel.

Hvorfor er dette viktig: En god sikkerhetskultur bidrar til at virksomhetens sikkerhetstiltak ivaretas av medarbeiderne. Dersom medarbeiderne vet hva som er forventet av dem, tar ansvar for egne handlinger og har en forståelse for hvorfor sikkerhetstiltak eksisterer, vil de også sørge for å melde fra om sikkerhetsmessige forhold som virksomheten bør vite om.

Anbefalte tiltak:

- Implementer og oppretthold rutiner for rapportering og sårbarhetsoppfølging.
- Skap en aksept og forståelse hos medarbeiderne for hvorfor sikkerhets- og kontrollrutiner eksisterer.
- Lær medarbeiderne om viktigheten av rapportering.
- Legg til rette for en åpen tilbakemeldingskultur.
- Fremhev og belønn positiv sikkerhetsatferd.
- Motiver medarbeiderne til å øke egen kompetanse innen sikkerhet.
- Gi orienteringer og hold obligatoriske oppfølgingskurs om ulike sikkerhetsutfordringer, eksempelvis sosial manipulasjon, trusselbildet og trusselen fra innsidere.
- Lag jevnlige kampanjer for å øke medarbeidernes sikkerhetsmessige bevissthet.
- Legg til rette for at den enkelte medarbeider former en kulturell identitet til virksomheten.
- Gjennomfør øvelser innenfor personellsikkerhet.

3.2. Ivareta medarbeidere gjennom tilpasset oppfølging

Tilpasset oppfølging av den enkelte medarbeider er en sentral del av virksomhetens arbeid for å ivareta og styrke personellsikkerheten. Dette fordi tilpasset oppfølging kan forebygge, avdekke og motvirke misnøye på arbeidsplassen og andre forhold ved den enkelte som kan svekke personellsikkerheten. Samtidig øker det muligheten for at virksomheten oppdager nye og aktualiserte forhold, for deretter å kunne implementere risikoreducerende tiltak.

Hvorfor er dette viktig: En tilpasset oppfølging av den enkelte medarbeider kan bidra til å øke trivsel, lojalitet og tillit til virksomheten og den enkeltes sikkerhetsmessige robusthet.

Anbefalte tiltak:

- Ivareta medarbeiderne gjennom oppfølging tilpasset den enkeltes forutsetninger og behov.
- Lytt til medarbeiderne og sørg for at det finnes arenaer hvor medarbeiderne kan uttrykke seg.
- Lær medarbeiderne om sårbarheter som kan være av sikkerhetsmessig betydning for virksomheten og be dem om å melde fra om relevante endringer i egen livssituasjon.
- Skap en åpen kommunikasjon med den enkelte medarbeider, slik at medarbeideren vil gå til leder dersom noe skjer.
- Sørg for en individuell oppfølging av den enkelte medarbeider ved endringer i virksomheten eller endring av arbeidsoppgaver.
- Sørg for en individuell oppfølging av den enkelte medarbeider dersom medarbeideren opplever endringer i livssituasjonen som vil kunne påvirke personen.

3.3. Følg opp medarbeidere med identifiserte sårbarheter

Medarbeidere med identifiserte sårbarheter bør følges opp gjennom ansettelsesforholdet. Dersom en medarbeider har sårbarheter ved seg, bør lederen implementere tiltak for å redusere sårbarheten til et akseptabelt nivå. Valg av tiltak bør gjøres på bakgrunn av den enkeltes situasjon hva gjelder sårbarheter og risiko forbundet med dens stilling eller oppdrag.

Hvorfor er dette viktig: Personellsikkerhetsmessige sårbarheter er forhold som vil kunne lede til ubevisst innsidevirksomhet og/eller utnyttes av en trusselaktør. Det er derfor viktig at virksomheten følger opp identifiserte sårbarheter og implementerer tiltak for å redusere risikoen.

Anbefalte tiltak:

- Avhold jevnlig samtaler med medarbeidere som har identifiserte sårbarheter.
- Øk den enkelte medarbeiders sikkerhetsmessige bevissthet ved å lære medarbeideren om implikasjonene ved det å inneha sårbarheter, hvordan det kan håndteres, og viktigheten av å melde fra om eventuelle endringer.
- Sørg for en åpen dialog mellom leder og den enkelte medarbeider for å senke terskelen for selvrapporing.
- Implementer andre sårbarhetsreducerende tiltak der dette er nødvendig for å redusere risikoen til et akseptabelt nivå – for eksempel en tettere oppfølging eller begrensinger i medarbeiderens ansvarsområder og tilgang til informasjon.
- Sørg for at leder eller andre med ansvar for å følge opp sårbarheter har tilstrekkelig kompetanse.

3.4. Avdekk nye personellsikkerhetsmessige sårbarheter

Under et ansettelsesforhold kan det oppstå nye sårbarheter hos den enkelte medarbeider. Nye sårbarheter kan både oppstå som følge av endringer i medarbeiderens liv, endringer i virksomheten eller endringer i trusselbildet. Misnøye på arbeidsplassen og avtagende sikkerhetsmessig bevissthet er eksempler på sårbarheter som kan oppstå etter at en medarbeider har fått tilgang til virksomhetens verdier.

Hvorfor er dette viktig: Avdekking av nye sårbarheter hos medarbeiderne er nødvendig for at virksomheten skal ha tilstrekkelig oversikt over eget risikobilde og være i stand til å innføre sårbarhetsreducerende tiltak.

Anbefalte tiltak:

- Implementer rutiner for identifisering og oppfølging av nye personellsikkerhetsmessige sårbarheter.
- Sikre at leder er oppdatert på det aktuelle trusselbildet og hva dette kan medføre for oppfølging av medarbeiderne.
- Påse at leder eller andre med ansvar for å følge opp nye sårbarheter håndterer informasjon som medarbeidere meddeler om endringer i egen livssituasjon.
- Øk medarbeidernes sikkerhetsmessig bevissthet gjennom informasjon rundt sårbarhet og risiko, og vurder tiltak for å redusere sårbarheten til et akseptabelt nivå.
- Sørg for å skape en forståelse hos medarbeiderne om nødvendigheten av å melde fra om vervingforsøk, tilnærminger og annen sikkerhetstruende kontakt.

3.5. Avklar årsaken til endringer i medarbeidernes atferd

Virksomheten bør ha tilstrekkelig evne og mulighet til å oppdage innsidevirksomhet og annen uønsket atferd blant medarbeiderne der dette kan få betydning for sikkerheten. Endringer i atferd kan være en indikator som bør undersøkes nærmere. Det er i denne sammenheng svært viktig å få avklart årsaken til at det har skjedd en endring og omstendighetene rundt endringen.

Hvorfor er dette viktig: Å oppdage avvik på et tidlig tidspunkt er viktig for å forebygge at en medarbeider, med eller uten intensjon, utgjør en innsiderisiko eller på annen måte kan komme til å påvirke virksomhetens sikkerhetstilstand.

Anbefalte tiltak:

- Vær kjent med hvilke indikatorer som kan si noe om økt risiko for innsidevirksomhet.
- Implementer systemer som identifiserer endringer i atferd.
- Iverksett adgangskontroll, logging og eventuelt andre teknologiske barrierer.
- Avklar årsaken til endring i atferd og følg opp aktualiserte sårbarheter.
- Sikre at leder følger opp innrapporterte saker ved å undersøke omstendighetene rundt avvikene.

- Gjennomfør sårbarhetssamtale med medarbeideren det gjelder. Adresser problemstillingen og skap en dialog med medarbeideren.

3.6. Ivareta sikkerheten ved avvikling av arbeidsforhold

Medarbeidere som slutter i en virksomhet tar med seg virksomhetens kunnskap. Det er derfor viktig å utarbeide og implementere tiltak som ivaretar sikkerheten også etter at arbeidsforholdet er avviklet. Videre bør det være et mål for virksomheten at medarbeidere som slutter, forlater virksomheten med et positivt inntrykk.

Hvorfor er dette viktig: Virksomheter med fokus på å ivareta sikkerheten ved avvikling kan redusere risikoen for at tidligere medarbeidere kompromitterer sensitiv informasjon om dens verdier eller sårbarheter. Personellsikkerhetsmessige tiltak bør ta sikte på å forebygge både bevisst og ubevisst kompromittering.

Anbefalte tiltak:

- Følg sjekklister og rundeskjemaer som sikrer at medarbeideren returnerer utlevert utstyr.
- Sørg for at medarbeiderens tilganger til informasjon, systemer, prosedyrer og adgang til objekter eller infrastruktur sperres, fjernes og/eller slettes.
- Informer kunder og andre aktuelle samarbeidspartnere om avviklingen av arbeidsforholdet. Informer samtidig om ny kontaktperson.
- Gjennomfør en egen avslutningssamtale om sikkerhet med de som slutter. Avklar årsaken til at personen slutter og følg opp eventuell misnøye.
- Vurder om det er nødvendig med umiddelbar avslutning av arbeidsoppgaver og sperring av tilgang/adgang.
- Sørg for at medarbeidere som forlater virksomheten eller avslutter et oppdrag forstår at taushetserklæringen som gjaldt under arbeidsforholdet, også gjelder etter avvikling.

4. Håndtere og gjenopprette

Denne kategorien omhandler håndtering av sikkerhetsrelaterte hendelser som involverer medarbeidere, det være seg en innsidesak, sikkerhetsbrudd eller annen bekymringsfull atferd der dette relateres til personellsikkerhetsmessige forhold. Formålet er at virksomheten skal være rustet til å håndtere slike situasjoner. Prinsippene i denne kategorien går ut på å vurdere, kontrollere og minimere skaden som allerede har skjedd, men også å forbedre personellsikkerheten basert på erfaringer.

4.1. Håndter hendelser proporsjonalt

Hvordan virksomheten bør håndtere hendelser avhenger av hendelsens alvorlighetsgrad. Det vil for eksempel være forskjell på hvordan virksomheten bør håndtere en innsidesak og et mindre sikkerhetsbrudd. Virksomheten bør være oppmerksomme på at generelle og spesifikke lover og regelverk vil kunne sette begrensninger for hendeshåndteringen, for eksempel regelverk som omhandler personvern.

Hvorfor er dette viktig: En proporsjonal håndtering er viktig for å sikre at alvorlige sikkerhetstruende hendelser blir håndtert deretter. Man ønsker også å unngå unødvendig eskalering av mindre alvorlige hendelser. Dersom medarbeiderne opplever at hendelser håndteres riktig ut ifra alvorlighetsgrad, vil dette kunne bidra til å skape en god sikkerhetskultur.

Anbefalte tiltak:

- Få en oversikt over hva som har skjedd og hvem som har vært involvert.
- Foreta en første vurdering av hendelsens skadefølger og årsaken(e) til hendelsen.
- Håndter hendelsen uten unødig opphold. Vurder tverrfaglig samarbeid.
- Identifiser hvilken rolle involvert(e) person(er) har/har hatt.
- Vurder å snakke med medarbeideren – gi personen(e) muligheten til å fortelle/forklare.
- Iverksett tiltak proporsjonalt til hendelsen, for eksempel en bevisstgjørende samtale med medarbeideren dersom det er snakk om et mindre alvorlig sikkerhetsbrudd.
- Vurder behovet for en strengere håndtering ved gjentatte og mer alvorlige hendelser.
- Kontakt politiet eller søk råd hos NSM eller andre myndigheter når dette er nødvendig.

4.2. Begrens skadene så raskt og så mye som mulig

For å redusere skadeomfanget av en hendelse, er det viktig å begrense konsekvensene så raskt og så mye som mulig. Virksomheten bør alltid vurdere om det er aktuelt å iverksette personellsikkerhetsmessige tiltak, og i så fall hvilke.

Hvorfor er dette viktig: En rask og effektiv begrensning av konsekvenser etter en hendelse er viktig for å redusere skadeomfanget og gjenopprette et akseptabelt sikkerhetsnivå.

Anbefalte tiltak:

- Gjennomfør umiddelbare tiltak – for eksempel repetisjon av sikkerhetsprosedyrer og umiddelbare begrensninger i adganger og tilganger.
- Rapporter om hendelsen til berørte parter (både internt og eksternt). Prioriter raske tilbakemeldinger til aktører som kan bli berørt i stor grad.
- Følg kommunikasjonsplanen, internt og eksternt.
- Sørg for tett oppfølging av medarbeideren dersom det er kjent hvem som forårsaket hendelsen (husk proporsjonal håndtering).

- Legg en plan for hvordan en eventuell grundigere undersøkelse skal foregå, eksempelvis dersom det er ukjent hvem eller hva som har forårsaket hendelsen.
- Anmeld forhold ved mistanke om at virksomheten har blitt utsatt for et lovbrudd. Ved mistanke om spionasje fra fremmede stater må norske myndigheter varsles, og spionasje fra konkurrerende virksomheter bør anmeldes til politiet.

4.3. Ivareta medarbeiderne også under hendeshåndtering

Å håndtere det menneskelige aspektet ved uønskede hendelser, for eksempel der eget personell er involvert, kan være krevende avhengig av hendelsens alvorlighetsgrad. Virksomheten bør sørge for å utføre selve håndteringen på en god og lovmessig måte, og samtidig ivareta medarbeiderne – spesielt dersom granskning av hendelsen kan føre til konsekvenser for enkeltpersoner (anmeldelse, mistillit etc.).

Hvorfor er dette viktig: Samtidig som en hendelse håndteres, vil virksomheten ofte ønske å fortsette daglig drift. Det er da avgjørende at virksomheten ivaretar fokuset på sikkerheten for å gjenopprette akseptabelt sikkerhetsnivå. En sentral del av dette er å sørge for at medarbeiderne blir ivaretatt på best mulig måte. Dette kan trygge medarbeiderne og øke deres sikkerhetsmessige kompetanse – noe som igjen er med på å gjøre medarbeiderne til barrierer mot uønskede hendelser og situasjoner.

Anbefalte tiltak:

- Ivareta medarbeiderne på best mulig måte, både personer involvert i hendelsen og andre. Vær bevisst på at en hendelse, også en som håndteres på en god måte, kan få uheldige konsekvenser for medarbeiderne.
- Involver aktuelle parter, eksempelvis HR, sikkerhetsleder, juridisk avdeling, kommunikasjonsavdelingen, arbeidstakerforeningene og kriseteam.
- Informer medarbeiderne når dette er mulig. Vurder hvilken informasjon som kan deles og når. Dette kan bidra til å trygge medarbeiderne og unngå ryktespredning.
- Iverksett eventuelle andre tiltak som kan trygge medarbeiderne, for eksempel ekstra adgangskontroll.
- Ytterligere autorisasjonsskille kan innføres for at en eventuell mindre gruppe skal kunne sikre videre drift.
- Følg prosedyre for mediehåndtering.

4.4. Evaluer hendelser og håndteringen av dem

Virksomheten bør evaluere hendelser og benytte evalueringen i det videre sikkerhetsarbeidet for å hindre gjentagelse. Virksomheten bør i tillegg foreta en vurdering av hvordan hendelser har blitt håndtert. En gjennomgang av tiltak som ivaretar personellsikkerheten er i seg selv et virkemiddel som kan bidra til å styrke sikkerheten. Leder har et overordnet ansvar for at det gjennomføres evalueringer.

Hvorfor er dette viktig: Evalueringer av hendelser og håndteringen av dem er viktig for å identifisere forbedringspunkter og løfte sikkerhetsarbeidet i virksomheten.

Anbefalte tiltak:

- Involver relevante aktører i evalueringsarbeidet, eksempelvis HR (personalavdelingen), sikkerhetsleder, datasikkerhetsleder og personellsikkerhetsansvarlig.
- Sørg for at det avholdes en debrief med de involverte partene og en objektiv tredjepart.³ Debrief bør gjennomføres så snart som mulig. Ved behov bør man også gjennomføre en emosjonell debrief, der hendelsen og håndteringen kan bearbeides.
- Gjennomfør evalueringen så snart det er hensiktsmessig og forsøk å få frem et helhetlig bilde. Ved behov bør evalueringen gjennomføres av en objektiv tredjepart.
- Dersom det forelå innrapportering – vurder hva/om man kunne håndtert det annerledes.
- Utarbeid en skriftlig evalueringsrapport.
- Be om tilbakemeldinger fra medarbeiderne der dette er naturlig – for eksempel ved større hendelser.

4.5. Lær av erfaringer og implementer endringer

Virksomheten bør arbeide systematisk for å lære av egne erfaringene og bruke lærdommen til å styrke sikkerhetsarbeidet. Det er viktig å bruke nok tid og ressurser på å lære av hendelser. Fullstendig gjenopprettelse av et forsvarlig sikkerhetsnivå vil først skje etter evaluering og implementering av tiltak som skal hindre at noe lignende kan skje igjen. Virksomheten bør også etterstrebe å lære av andre virksomheters erfaringer når dette er mulig.

Hvorfor er dette viktig: Det å lære av erfaringer og implementere nødvendige endringer er viktig for at virksomheten skal kunne forbedre egen evne til å håndtere hendelser og hindre at samme eller lignende hendelse vil skje igjen. Gjennom erfarings- og kunnskapsbaserte endringer kan man styrke virksomhetens robusthet mot sikkerhetstruende hendelser.

Anbefalte tiltak:

- Sikre at erfaringer deles på tvers av virksomhetens avdelinger der dette kan bidra til læring og styrking av personellsikkerheten (husk å ta hensyn til relevante lov- og regelverk).
- Ta sikte på å dele egne erfaringer og lære av andre virksomheters erfaringer.
- Innarbeid eventuelle endringer i planverket.
- Etabler permanente korrigerende tiltak for å hindre gjentagelse.
- Evaluer om virksomhetens korrigerende tiltak fungerer som forutsatt.

³ Person/funksjon i virksomheten som kjenner til rutine og som ikke har vært en aktiv part i hendelsesforløpet/forholdet/selve håndteringen. Dette kan for eksempel være sikkerhetsleder eller deler av øvrig ledelse.

**Nasjonal
sikkerhetsmyndighet**

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no