Sikkerhet ved ansettelsesforhold

- før, under og ved avvikling

Utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd

Forord

Offentlige myndigheter ved PST, NSM, Økokrim og Kripos har gjennom flere år og i ulike trusselvurderinger og rapporter, pekt på innsidetrusler som en utfordring for både offentlige og private virksomheter. Nasjonalt og internasjonalt ser en at etablerte forretningsstrukturer og strategisk viktige ansatte korrumperes og at sårbarheter blir gjenstand for kriminalitet. Dette med risiko for tap av store verdier både i privat og offentlig sektor. Denne alvorlige samfunnstrusselen krever økt oppmerksomhet.

Aktuelle myndigheter har sammen med Næringslivets Sikkerhetsråd (NSR), utarbeidet denne veilederen som forhåpentligvis vil gi en økt bevissthet rundt trusselen. I tillegg ønsker vi at veilederen vil bidra til å sette virksomhetene bedre i stand til å foreta gode valg og ha gode rutiner både før, under og ved avvikling av ansettelsesforhold samt ved innleie av ulike tjenester.

Innhold

1 Formål og bakgrunn

Formålet med denne veilederen er å gi offentlige og private virksomheter et hjelpemiddel de kan bruke når de skal planlegge tiltak for å redusere risikoen som innsidervirksomhet kan representere.

Veilederen har en helhetlig tilnærming og foreslår en rekke tiltak, som må utføres systematisk og i riktig rekkefølge. Dette innebærer at virksomheten må fokusere på personellsikkerhet både før de ansetter noen, under ansettelsesforholdet og når forholdet avvikles.

Veilederen kan være til nytte for både private og offentlige virksomheter. Det understrekes at veilederen ikke skal benyttes i tilfeller der sikkerhetsloven stiller krav til sikkerhetstiltak overfor ansatt personell. I disse tilfeller er det kravene i lov og forskrift, med egne veiledninger som er gjeldende.

Vi understreker at når virksomheten skal gjennomføre personellsikkerhetstiltak må den forsikre seg om at tiltakene ikke strider mot lover og regler om personvern og arbeidstakers rettigheter.

Veilederen er delt inn slik at den følger en ansettelsesprosess fra stillingen lyses ut til arbeidsforholdet avvikles. Deretter omtaler den personellsikkerhetstiltak ved bruk av konsulenter og annen innleid arbeidskraft.

Veilederen berører også kort hvordan virksomheten bør forholde seg når de bruker en tredjepart til å gjennomføre en bakgrunnssjekk, og hvordan de bør vurdere opplysninger som fremkommer i en slik sjekk.

Selv om veilederen tar en helhetlig tilnærming, er ikke listen over foreslåtte tiltak å anse som uttømmende. En virksomhet som iverksetter disse tiltakene, vil imidlertid kunne redusere sin risiko knyttet til personellsikkerhet. Veilederen legger opp til at personellsikkerhet gjøres til en integrert del av virksomhetens øvrige sikringstiltak.

Det er viktig at alle tiltak som iverksettes er i tråd med gjeldende regelverk. Noen virksomheter har egen lovhjemmel for gjennomføring av bakgrunnssjekk av søkere før en ansettelse. Disse kan trolig gå lenger i sine undersøkelser enn en virksomhet uten slik hjemmel. Det er også viktig at virksomheten skiller mellom aktiviteter som kan gjøres før en ansettelse og aktiviteter knyttet til personer som allerede er ansatt.

1.1 Trusselen

Et ansettelsesforhold forutsetter et betydelig tillitsforhold mellom den ansatte og arbeidsgiver, ettersom arbeidsgiveren gir den ansatte tilgang til virksomhetens verdier. Når arbeidsforholdet avsluttes, tar den ansatte dessuten med seg all kunnskapen han eller hun har ervervet.

I dagens arbeidsliv er bruken av midlertidig arbeidskraft utbredt, enten det dreier seg om midlertidig ansatte, konsulenter eller kontraktører. Uavhengig av lengden på ansettelsesforholdet må disse gruppene ofte vises samme tillit som virksomhetens egne ansatte. De tar også med seg kunnskapen de har fått, når de ikke lenger arbeider for virksomheten. Det samme gjelder for personer som kun er ansatt en kort periode.

Kombinasjonen av kunnskap og tillit gjør at en nåværende eller tidligere ansatt har store muligheter for å skade virksomheten ved å misbruke tilliten han eller hun er vist. I noen tilfeller gjøres det med overlegg, mens andre ganger kan den ansatte skade virksomheten fordi han eller hun ikke forstår eller evner å følge rutinene som skal sikre virksomhetens verdier. Konsekvensene for virksomheten kan for eksempel være økonomisk tap, tap av forretningshemmeligheter eller sensitiv informasjon på avveie eller et svekket renommé.

Denne veilederen definerer en innsider som *«en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap»*[1] .

I sin ytterste konsekvens kan en innsider medvirke til eller gjennomføre spionasje, sabotasje eller terrorhandlinger som kan resultere i at samfunnskritiske funksjoner blir satt ut av spill, eller i at liv og helse blir satt i fare.

En ansatt som handler i strid med virksomhetens interesser, har derfor et stort skadepotensial. Virksomhetens ansatte er dermed ikke bare en ressurs, men utgjør fra et personellsikkerhetsmessig ståsted også en potensiell sårbarhet og i noen tilfeller en trussel mot virksomheten. Dette gjelder også tidligere ansatte, innleide konsulenter og kontraktører.

1 Australia Government Managing The Insider Threat To Your Business - A personnel security handbook

Blant aktørene som kan tenkes å benytte innsidere, er andre staters etterretnings- og sikkerhetstjenester, konkurrerende virksomheter, kriminelle miljøer og terrororganisasjoner. Men en innsider kan like gjerne handle på eget initiativ, og ikke arbeide for en tredjepart. Innsidervirksomhet kan rette seg mot alt fra kritisk, samfunnsviktig informasjon til pengene i kassaapparatet. Det er viktig å understreke at det er en rekke andre sikringstiltak som bør iverksettes i tillegg til de personellsikkerhetsmessige, og at det er samspillet mellom alle disse tiltakene som gir god beskyttelse. Dersom virksomheten faller inn under sikkerhetsloven, er det krav om iverksettelse av tiltak på ulike områder.

Innsidere kan deles inn i tre kategorier. Den første er infiltratøren. Infiltratøren er plassert i virksomheten av en tredjepart som ønsker å utnytte tilgangen han gis, på en måte som skader virksomheten. Den andre er den selvmotiverte, ondsinnede innsideren, som gjennomfører den tilsiktede uønskede handlingen på eget initiativ og i utgangspunktet ikke har kontakt med eller styres av en tredjepart. Den tredje kategorien er den rekrutterte innsideren, som jobber frivillig eller under press for en tredjepart. Rekrutteringen skjer ofte etter at personen har fått tilgang til virksomhetens verdier. I tillegg har man den som uforvarende som uten å forstå det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet eller har ikke kompetanse til å forstå konsekvensene av handlingen sin.

En uttømmende liste over hva som kan motivere noen til å bli en innsider, kan ikke utarbeides. Noen forklarende faktorer som ofte trekkes frem, er imidlertid misnøye med arbeidsgiver, økonomi, personlige problemer, ønsker om hevn, arbeidsrelaterte problemer, delt lojalitet, søken etter spenning, sårbarheter som gjør at vedkommende kan presses, og manglende opplæring, sikkerhetsrutiner eller personlig sikkerhetsmessig dømmekraft.

2 Virksomhetens styrings-system for sikkerhet

Virksomheten må sette sikkerhetsarbeidet i system, både for å få oversikt over sikkerheten generelt og for å kunne opprettholde en tilfredsstillende sikkerhetstilstand over tid. Systemet bør omfatte systematiske og kontinuerlige prosesser for helhetlig å planlegge, drifte, evaluere og forbedre arbeidet med sikkerhet. Systemet bør dessuten ses i sammenheng med organisasjonen og virksomhetsstyringen for øvrig.

For at virksomheten skal kunne håndtere sårbarheter som mennesker kan utgjøre, er det viktig at arbeidet med personellsikkerhet er en tydelig del av styringssystemet for sikkerhet.

Tenk over:

- Har vi et velfungerende styringssystem for sikkerhet?
- Er personellsikkerheten en tydelig del av dette systemet?
- Har vi identifisert nøkkelpersonell og nøkkelstillinger?
- Har vi identifisert hvilken risiko en ansatt kan utgjøre for oss?
- Er ledelsen klar over denne risikoen?

Et helhetlig styringssystem for sikkerhet handler i hovedtrekk om fire forhold:

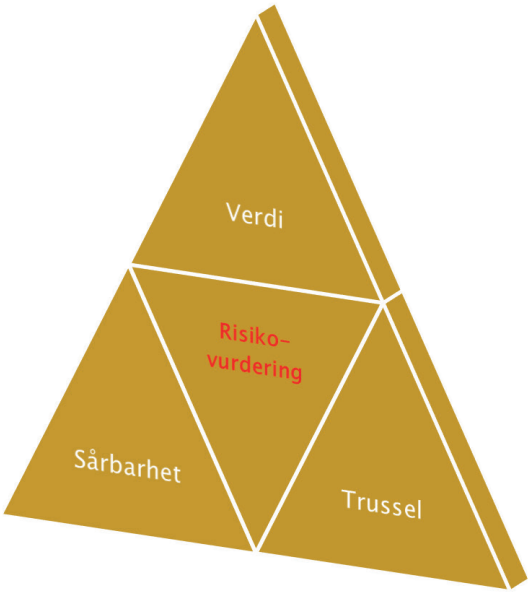
- lederforankring
- en strukturert metode for sikkerhetsarbeidet
- organisering og roller
- nødvendig dokumentasjon og nedfelte rutiner

2.1 Sikkerhetskultur

Alle virksomheter bør tilstrebe å ha en god sikkerhetskultur. En slik kultur innebærer blant annet:

- forankring både i ledelsen og hos de ansatte
- god sikkerhetsatferd både blant ledelsen og blant de ansatte
- at ledelsen kommuniserer og begrunner behovet for sikkerhetstiltak
- aksept, forståelse og bevissthet rundt personellsikkerhetstiltakene hos de ansatte
- eierskap til tiltakene hos de ansatte, gjerne gjennom god opplæring og informasjon
- at tiltakene etterleves og er en integrert del av hele virksomheten
- tilgang til sensitiv informasjon bare for personer med dokumentert behov

NSMs veileder i sikkerhetsstyring



Norsk standard - Sikringsrisikoanalyse 5832: 14

- at den enkelte erkjenner at egen atferd påvirker sikkerheten
- etterlevelse av regler og prosedyrer for personellsikkerhet
- at sikkerhetsbrudd rapporteres
- at det oppmuntres og legges til rette for at ansatte kan komme med forslag til forbedringer av sikkerhetsarbeidet

2.2 Risikovurdering

Det er viktig at virksomheten foretar en strukturert gjennomgang av hvilke verdier den besitter. Både informasjon og objekt kan være av stor betydning for en virksomhet. Dette vil være grunnlaget for hva som bør beskyttes mot eventuelle innsidere. Deretter må virksomheten foreta en risikovurdering der man får tydeliggjort hvilken risiko den konkrete virksomheten står overfor. Dette vil være utgangspunktet for arbeidet med personellsikkerhet i virksomheten.

- Kartlegg verdier i virksomheten
- Foreta en enkel risikovurdering av hva feilansettelser kan medføre.
- Identifiser hvilke stillinger eller oppgaver som er spesielt utsatte.
- Utarbeid rutiner for bakgrunnssjekk for de aktuelle stillingene.
- Beslutt hvem i virksomheten som har det overordnede ansvaret for bakgrunnssjekker.
- Sørg for at informasjon og skjemaer er tilgjengelig for aktuelle personer.

Virksomheten bør også vurdere om det skal gjennomføres samme type bakgrunnssjekk for alle ansatte, eller om noen stillinger skal kreve en mindre eller mer omfattende sjekk. Videre bør virksomheten avklare om personer som skifter stillinger internt, skal sjekkes på nytt. Man kan eventuelt ha en egen type bakgrunnssjekk for slike tilfeller. Det er avgjørende at virksomheten foretar en grundig vurdering av behov, muligheter og begrensninger før de innfører tiltak. En god plan er ofte et godt suksesskriterium.

2.3 Rutiner og prosedyrer

Personellsikkerhet må forankres i ledelsen, som alle andre sikkerhetsfremmende tiltak. Det bør utarbeides en prosedyre/rutine for bakgrunnssjekk. Prosedyren bør være skriftlig for å sikre notoritet, og må være i tråd med gjeldende regelverk om likestilling, antidiskriminering, HMS og krav til offentlighet og privatlivets fred. I tillegg må virksomheten være åpen overfor de ansatte og aktuelle kandidater om at de gjennomfører bakgrunnssjekk, og om årsakene til at de gjør det.

Dette forankrer bakgrunnssjekken som en del av virksomhetens rekrutteringsprosess og sikkerhetskultur.

Punktene under viser hva prosedyrene og rutinene bør omfatte.

2.3.1 Intern ansvarsfordeling

- Hvem har det overordnede ansvaret for bakgrunnssjekken?
- Hvem gjennomfører bakgrunnssjekken?
- Hvem foretar den endelige vurderingen?

2.3.2 Informasjonsinnhenting

- Hvem skal hente inn informasjonen?
- Hvordan skal informasjonen hentes inn?
- Hva slags informasjon skal hentes inn?
- Hvilken informasjon skal søkes verifisert?
- Hvordan skal den verifiseres – skal den dokumenteres, kontrolleres i elektroniske kilder eller skal mennesker kontaktes?
- Hvilken informasjon kan ikke verifiseres?

2.3.3 Vurdering

- Hvordan skal informasjonen fra bakgrunnssjekken vurderes?
- Hva er akseptabel risiko for virksomheten? (må sees i lys av risikovurderingen)

2.3.4 Informasjonsbehandling

- Personopplysningslovens krav må tilfredsstilles
- Hva er hjemmelsgrunnlaget for behandlingen av opplysningene?
- Hva er formålet med behandlingen?
- Hvem skal ha tilgang til opplysningene fra bakgrunnssjekken?
- Hvordan skal opplysningene sikres?
- Hvor lenge skal opplysningene lagres?
- Hvordan skal opplysningene makuleres?

2.3.5 Annet

- Hvilke stillinger omfattes av bakgrunnssjekken?
- Skal en tredjepart gjennomføre bakgrunnssjekken eller deler av den?
- Den skriftlige prosedyren bør underlegges versjonsstyring for å sikre notoritet.
- Prosedyrene og rutinene må godkjennes og signeres av virksomhetens leder, styret eller den med formelt delegert myndighet fra ledelsen, med sted og dato.

For å sikre likebehandling, effektivitet og konfidensialitet for bakgrunnssjekker bør én person gis hovedansvaret for gjennomføringen av dem. Virksomheten bør sørge for at denne personen har tilstrekkelig kunnskap om hvordan en slik prosess bør gjennomføres.

I tillegg til opplysningene personen som vurderes ansatt oppgir i jobbsøknaden, kan virksomheten be hun eller han fylle ut et eget personopplysningsskjema for å sikre seg tilstrekkelig informasjon til å gjennomføre bakgrunnssjekken.

Et slikt skjema kan inneholde:

- fullt navn, inkludert tidligere navn
- fødselsdato og -år
- nåværende og tidligere adresser med dato og årstall
- utdannings- og ansettelseshistorikk med dato og årstall
- informasjon om at det vil bli gjennomført en bakgrunnssjekk og opplysninger om konsekvensene av å oppgi feilaktige opplysninger
- kandidatens bekreftelse på og samtykke i at det vil bli gjennomført en bakgrunnssjekk
- en tillatelse til å hente inn informasjon fra for eksempel tidligere arbeidsgivere, kredittinstitusjoner og andre
- et eget felt for utfyllende opplysninger fra kandidaten

3 Bakgrunnssjekk før en ansettelse

3.1 Hva er bakgrunnssjekk?

Før en ansettelse bør virksomheten gjennomføre en bakgrunnssjekk. Dette er prosessen med å innhente, sammenligne og dokumentere informasjon om en person, i den hensikt å bekrefte eller avkrefte det kandidaten selv opplyser. Den kan også omfatte datainnhenting eller søk i åpne kilder (kredittsjekk, søk på næringsinteresser, i adresseregistre osv.).

Formålet med bakgrunnssjekken er todelt. For det første gir den virksomheten mulighet til å forsikre seg om at opplysningene kandidaten oppgir under ansettelsesprosessen, er korrekte, enten det dreier seg om bevisste løgner eller misforståelser. For det andre virker bakgrunnssjekken forebyggende. Gjennomføres den på en god måte, kan den redusere sannsynligheten for å ansette personer som har sårbarheter, og som enten på ansettelsestidspunktet eller senere vil utgjøre en trussel mot virksomhetens verdier.

Dette forutsetter at funnene i en bakgrunnssjekk vurderes opp mot kriteriene i virksomhetens risikovurdering, og at det endelige resultatet samsvarer med det akseptable risikonivået i virksomheten. Dersom det er stor usikkerhet knyttet til en kandidat, og usikkerheten er sett i forhold til de verdiene virksomheten ønsker å beskytte, må dette få konsekvenser for den videre ansettelsesprosessen. Virksomheten må vurdere om det kan iverksettes kompenserende tiltak overfor denne personen, eller om vedkommende er uønsket i virksomheten. Dette må tydeliggjøres overfor kandidatene tidlig i ansettelsesprosessen.

Bakgrunnssjekken bør gjennomføres før den som skal ansettes gis adgang til virksomhetens lokaler, prosedyrer og informasjonssystem. En bakgrunnssjekk er både inngripende og kostbar og bør derfor stå i forhold til verdiene vedkommende vil få tilgang til.

3.2 Bakgrunnssjekkens innhold

Bruk gjerne kandidatens CV som grunnlag for å beslutte hva som skal undersøkes, og hvordan.

En bakgrunnssjekk kan deles inn i fire hoveddeler:

- identitetskontroll
- verifisering av utdanning og arbeidserfaring
- kredittsjekk og sjekk av næringsinteresser
- søk i åpne kilder

Denne veilederen fokuserer på disse hovedpunktene, men hver enkelt virksomhet må etablere og implementere egne instrukser og rutiner tilpasset sine behov.

3.2.1 Ved rekruttering

Under en ansettelsesprosess er virksomheten først og fremst opptatt av å finne den beste kandidaten til stillingen, men dersom stillingen inngår i virksomhetens risikoportefølje er det viktig å tenke sikkerhet allerede på dette tidspunktet.

Gjør det kjent allerede i stillingsutlysningen at det vil kunne bli foretatt en bakgrunnssjekk tilpasset stillingens karakter. Bakgrunnssjekken bør gjennomføres før kandidaten kalles inn til intervju.

3.2.1.1 Samtykke fra kandidaten

Samtykket er jobbsøkerens aksept av at de aktuelle undersøkelsene utføres. Regler finnes i personopplysningsloven § 2 nr. 7. Husk at det er frivillig å gi et slikt samtykke. Velger kandidaten å avslå, kan ikke bakgrunnssjekken iverksettes som skissert i denne veilederen.

Samtykket må være skriftlig og er ofte en forutsetning for å få opplysninger fra kilder som universiteter, skoler og tidligere arbeidsgivere, og især fra offentlige aktører og offisielle registre.

Samtykkeskjemaet bør som et minimum inneholde opplysninger om:

- hvem som utfører bakgrunnssjekken
- hva hensikten er, og hva resultatene skal brukes til
- hvilken informasjon som vil bli verifisert
- hvilke kilder som vil bli kontaktet
- personvernlovgivningen og kandidatens rettigheter
- hvor og hvordan opplysningene skal lagres

3.2.2 I*dentitetskontroll og oppholdstillatelse*

Bruk av falske identiteter er et stort problem, også i Norge. Det er en utfordring for samfunnet å få klarhet i hvem som oppholder seg og arbeider i Norge til enhver tid. Falske, fiktive, stjålne og lånte identiteter har vært benyttet til å søke jobb i både offentlig og privat sektor.

3.2.2.1 *Verifisering av fremlagte identitetsdokumenter*

- Be alltid kandidatene, uansett landtilhørighet, om å ta med seg nasjonalt pass til intervjuet og til første arbeidsdag.
- Sjekk identitetsdokumentet nøye. Det er avgjørende å få verifisert at jobbsøkeren er den han eller hun utgir seg for å være.
- Bruk enkelt utstyr som UV-lys og forstørrelsesglass
- Sammenlikne gjerne dokumentet med åpne referansedatabaser som f.eks Edison TD www.edisontd.net eller Prado ved www.consilium.europa.eu/prado

En grunnleggende personkontroll bør inneholde

- Sammenlikning av foto på dokumentet med kandidaten
- En samtale med kandidaten om dokumentet og identitetsopplysningene ved å stille åpne spørsmål.

3.2.2.2 *Utenlandske søkere*

Jobbsøkeren må ha gyldig opphold i Norge. Virksomheten kan søke utlendingsmyndighetene UDI (www.udi.no) eller politiet (Politiets utlendingsenhet eller lokalt politi) om bekreftelse.

- Husk at EU- og EØS-borgere ikke trenger å søke om opphold i Norge. Det er imidlertid identitetsdokumenter fra disse landene som er attraktive å inneha.
- For andre enn EU- og EØS-borgere (tredjelandsborgere) bør man særlig finne ut når en midlertidig oppholdstillatelse (studie- eller arbeidstillatelse) går ut.

3.2.3 *Verifisering av utdanning*

Norge
Be kandidaten gi deg tilgang til Vitnemålsportalen, der du finner karakterer og fullførte utdanninger, eller kontakt studiested direkte.

Du kan få svar på:

- studiets varighet (start- og sluttdato) samt om det ble tatt på fulltid eller deltid
- om studiet ble fullført eller ikke, og om kandidaten besto
- om kandidaten oppnådde en tittel eller grad, og i så fall hvilken
- om kandidatens vitnemål/karakterutskrift er korrekt

Er skolen nedlagt? Opplysninger fra offentlige skoler og universiteter ender til slutt i offentlige arkiver som by-, fylkes- eller statsarkiver.
Se www.arkivverket.no.

Andre land
NOKUT er det nasjonale kompetansesenteret for godkjenning av utdanning tatt i utlandet. Arbeidsgiver kan kreve å få se dokumentasjon på godkjenning.

- NOKUT utsteder godkjenningsdokumenter til personer som søker om å få vurdert sin utdanning fra utlandet. Dokumentet beskriver utdanningen sett i forhold til norsk høyere utdanning og angir omfanget i antall år og studiepoeng og eventuelt hvilken norsk grad utdanningen tilsvarer.
- NOKUT vurderer om dokumentene er ekte, og forsøker å verifisere dersom det er tvil.
- Dersom søkeren ikke har et slikt godkjenningsdokument, kan arbeidsgiver ved innkalling til intervju be han eller hun kontakte NOKUT for å få det tilsendt.

Du finner ytterligere informasjon på www.nokut.no/no.

Vitnemålsportalen er en ny digital tjeneste, utviklet på oppdrag fra Kunnskapsdepartementet. Ved hjelp av Vitnemålsportalen kan du selv hente ut dine resultater fra høyere utdanning og dele dem med studiesteder, potensielle arbeidsgivere og andre relevante parter. Tjenesten er gratis å benytte og har vært i drift siden januar 2017.

Tenk over: Kandidaten kan ha næringsinteresser som er konkurrerende til din virksomhet, og kan komme til å misbruke informasjon hun får tilgang til hvis hun blir ansatt. Dersom personen har slik næringsvirksomhet, bør det avklares nærmere.

3.2.4 *Verifisering av yrkeserfaring*

Samtaler med referansepersonene søkeren har oppgitt, er en subjektiv kontroll blant annet for å få bekreftet yrkeserfaringen i søkerens CV.

- Sjekk om den oppgitte referanseorganisasjonen er reell - i offentlige registre som Brønnøysundregistrene
- Kontroller at referansepersonen faktisk har jobbet sammen med kandidaten.
- Ring om mulig et telefonnummer som er koblet til et sentralbord, og ikke et mobiltelefonnummer.
- Ha gjerne en mal for samtalen som skal gjennomføres.
- Husk å innhente samtykke fra kandidaten i forkant.
- Snakk gjerne med både ledere, sideordnede og underordnede.
- Henvend deg til HR-avdelingen eller personalkontoret, eventuelt til avdelingen kandidaten jobbet ved.

Dersom sjekken gjelder yrkeserfaring, kan det lønne seg å stille følgende spørsmål:

- Hvor lenge varte arbeidsforholdet (start- og sluttdato)?
- Jobbet vedkommende fulltid eller deltid?
- Stemmer titler og funksjoner med det som er oppgitt i CV-en?

3.2.5 *Næringsinteresser*

Brønnøysundregistrene og for eksempel European Business Register (www.ebr.org) gir en oversikt over næringsinteresser og roller kandidaten har i virksomheter.

Mange av registrene tar betalt for søk og oppslag, og det kan lønne seg å inngå lisensavtaler for å få en lavere pris per søk.

Søk på vedkommende sine roller, knytninger til firma og andre næringsinteresser. Dette tilbys av ulike leverandører og av alle som tilbyr kredittsjekk.

3.2.6 *Kredittsjekk og økonomisk vandel*

Kredittsjekk i forbindelse med rekruttering kan foretas når det er saklig behov for det. Les mer i personopplysningsforskriften § 4-3. Virksomheten må i sine prosedyrer ha identifisert når kredittsjekk er relevant og i forhold til hvilke stillinger. Risikovurderingen bør angi hva som er et akseptabelt risikonivå, og bakgrunnssjekken må ta utgangspunkt i dette.

- Det må foretas en kvalitativ vurdering av om det kan og skal foretas en kredittsjekk, og søkeren må samtykke.
- Det er flere leverandører av tjenester for kredittsjekk i Norge.

NB: Det er ikke adgang til å lagre selve kredittvurderingen; kun resultatet kan noteres. Det betyr at eventuelle detaljer om betalingsanmerkninger, gjeld eller panteheftelser ikke skal lagres i personalarkivet eller tilsvarende.

3.2.7 *Søk i åpne kilder*

Husk at åpne kilder ofte inneholder uverifisert informasjon. Opplysninger herfra bør derfor ikke ekskludere kandidaten, men heller være tema under et eventuelt intervju.

- Søk etter informasjon om kandidaten i åpne kilder, for eksempel i ulike sosiale media
- Tjenester som samler informasjon om personer fra flere ulike kilder og gjør den tilgjengelig i én database, kan gjøre søket enklere.

NB: Ikke all informasjon på nettsider og i sosiale medier er korrekt og gir et riktig og sannferdig bilde av kandidaten. Vis kritisk sans, og bruk kun informasjon som er relevant for stillingen.

3.2.8 *Annen informasjon*

Andre elementer det kan være aktuelt å se på under bakgrunnssjekken:

- autorisasjoner, godkjenninger og tillatelser
- fagbrev og mesterbrev
- sertifikater og lisenser
- bevillinger og løyver
- helseattester – der dette er relevant for stillingen

3.2.9 Intervju

Intervjuet er et nyttig verktøy som kan gi et mer helhetlig inntrykk av kandidatens holdninger også når det gjelder sikkerhet, verdier og egne sårbarheter. Det gir også kandidaten mulighet til å vise at hun eller han har et bevisst forhold til disse temaene. Intervjuet kan også brukes til å oppklare uklarheter i dokumentasjonen. Den enkelte virksomhet må selv identifisere hvilke temaer som er relevante.

Informasjon som fremkommer i intervjuet, må nedtegnes slik at den kan etterprøves.

Spør om kandidatens bakgrunn, for eksempel om:

- oppvekst
- familie
- omgangskrets
- fritid

Ferdighetstest

En god måte å kontrollere at kandidaten har ferdighetene hun eller han har oppgitt i søknaden og CV-en, er å gjennomføre en test som kan gi et tydelig signal på om kompetansekravene er innfridd.

4 Under ansettelsesforholdet -Daglig sikkerhetsledelse

En sikkerhetsmessig atferd må sikres gjennom hele ansettelsesforholdet, og både ledere og den enkelte ansatte har ansvar for dette.

Sikkerhetsledelse av virksomhetens ansatte er en kontinuerlig prosess som følger den ansatte fra tiltredelse, gjennom hele ansettelsesforholdet og frem til forholdet avsluttes. Prosessen omfatter også tidligere ansatte, for eksempel gjennom taushetserklæringer.

Trening og bevisstgjøring av ansatte med henblikk på sikkerhet er et viktig element. Sikkerhetsarbeidet omfatter det å lære opp de ansatte, oppdatere kunnskapen deres og motivere dem til å handle i tråd med virksomhetens retningslinjer.

Eksempler på tiltak:

- et obligatorisk introduksjonsprogram som presenterer virksomhetens retningslinjer for sikkerhet
- jevnlige kampanjer for å øke de ansattes bevissthet rundt sikkerhet
- jevnlige oppdateringer og informasjon om virksomhetens sikkerhetsrisiko
- obligatoriske oppfølgingskurs om ulike sikkerhetsproblemer, som sosial manipulasjon og trusselen fra innsidere
- sikkerhet som tema i nyhetsbrev eller på intranett
- ansvarliggjøring av den enkelte ansatte når det gjelder behandling av informasjon, systemer, prosedyrer og objekter

4.1 Hvordan kan man avdekke uregelmessigheter?

Virksomheten bør ha tilstrekkelige muligheter til å avdekke innsidervirksomhet og annen uønsket atferd hos de ansatte. Blant annet bør den ha prosedyrer for hvordan ansatte og mellomledere kan varsle om bekymringer. Slike varsler kan gjelde uønsket atferd eller livsendringer av en slik art at de kan utgjøre en sårbarhet. De kan også gjelde atferd som indikerer at en ansatt opererer som innsider.

For å avdekke skadelig atferd er det viktig at ledere, mellomledere og ansatte er kjent med indikatorer på innsidervirksomhet og sosial manipulasjon.

4.2 Oppfølging av sårbarheter

Virksomheten bør ha ressurser og kompetanse til å følge opp sårbarheter som har oppstått hos ansatte. Oppfølgingen må være i tråd med gjeldende regelverk, og må ha som formål å redusere risikoen. Ved mistanke om at virksomheten er utsatt for et lovbrudd, bør forholdet anmeldes. Ved mistanke om spionasje fra fremmede stater må norske myndigheter varsles, og spionasje fra konkurrerende virksomheter bør anmeldes til politiet. Forhold ved ansatte som bør følges opp:

- misnøye
- atferdsendringer
- kontakt med kriminelle enkeltpersoner eller miljøer
- rus
- dårlig økonomi
- forbruk utover det inntekten skulle tilsi

Eksempler på konkrete temaer:

- Hvordan foregår sosial manipulasjon?
- Hva er innsidervirksomhet, og hvordan kan den foregå?
- Hvem er trusselaktørene mot virksomheten?
- Rutiner for behandling av informasjon, systemer, prosedyrer og objekter.

5 Avslutning av arbeidsforholdet

At en person slutter i en virksomhet, innebærer ikke nødvendigvis at han eller hun ikke lenger har noen forpliktelser overfor sin tidligere arbeidsgiver. Ansvar og forpliktelser som fortsatt gjelder etter at en ansatt har avsluttet eller endret sitt arbeidsforhold, som forpliktelser i henhold til en signert taushetserklæring, bør defineres og kommuniseres tydelig.

Prosedyrene knyttet til avslutning av et arbeidsforhold bør være en del av virksomhetens øvrige prosedyrer for personellsikkerhet. Sjekklister og rundeskjemaer kan brukes for å sikre at utlevert utstyr returneres. Prosedyren bør også inkludere at alle tilganger til informasjon, systemer, prosedyrer og objekter sperres og slettes elektronisk.

Eksempler på utstyr som bør leveres inn:

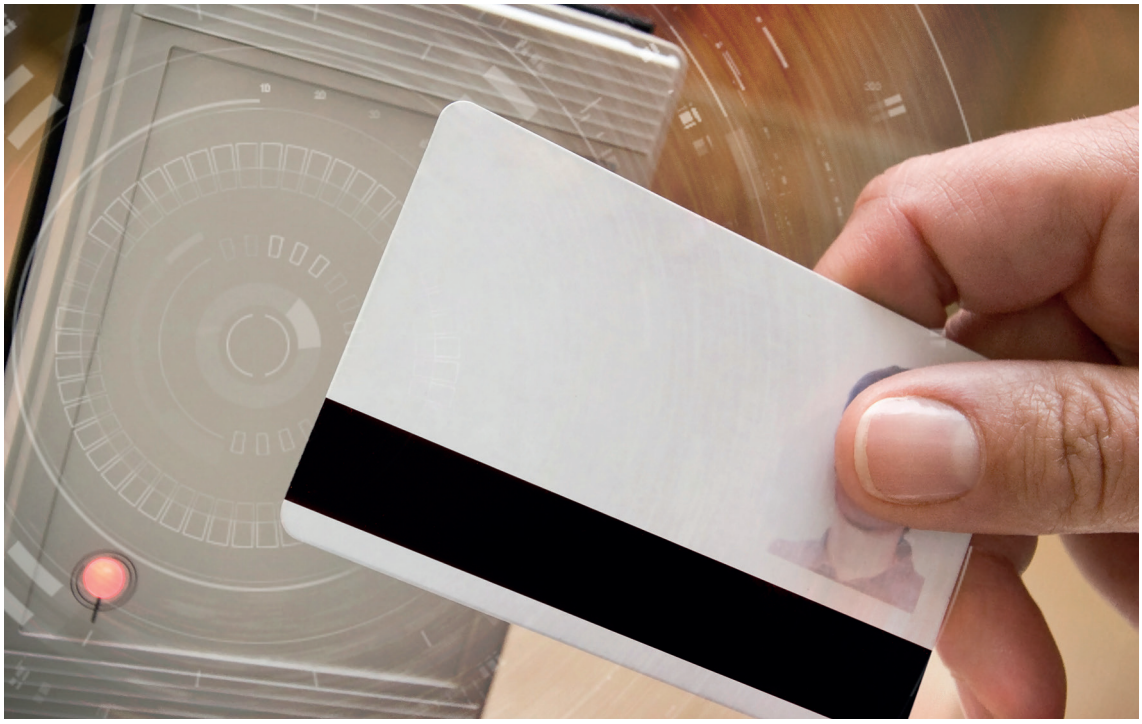
- adgangskort
- kodekort
- telefoner
- PC-er
- løse harddisker
- dokumenter
- USB-minnepinner
- nøkler

Eksempler på elementer som slettes elektronisk:

- passord
- koder
- brukerkontoer som benyttes til ekstern pålogging

Sørg for at kunder og andre samarbeidspartnere den som slutter har hatt kontakt med, vet at vedkommende nå slutter. Gi dem samtidig kontaktinformasjon til personen de skal forholde seg til fremover.

Gjennomfør en avslutningssamtale med den som slutter. Dette er spesielt viktig dersom vedkommende ikke selv har valgt å avslutte arbeidsforholdet.



6 Bruk av leverandører og konsulentselskaper

Både private og offentlige virksomheter har til tider behov for å bruke ulike leverandører og konsulentselskaper. Før man velger leverandør, bør man undersøke eierskap, struktur og historikk for å sikre at leverandøren har en etisk forsvarlig forretningsatferd og ikke forbindes med ulovlige eller uetiske handlinger.

Dette kan innebære å sjekke:

- Brønnøysundregistrene og lignende registre og databaser
- StartBANK
- leverandørens referansekunder

Prinsipielt vil alle forhold ved personellsikkerhet gjelde for leverandører og konsulenter på samme måte som for virksomhetens egne ansatte. Dette betyr at det sikkerhetsnivået som forventes innad i virksomheten, også skal forventes av leverandørene og konsulentene.

Virksomheten bør derfor tidlig i anskaffelsesprosessen definere sine sikkerhetskrav og beskrive disse i anbudsutlysninger og senere i avtaler med leverandører og eventuelle underleverandører. Da kan man unngå leverandører og konsulenter som ikke er egnet fra et sikkerhetsmessig ståsted.

Dersom man har behov for å innhente bistand fra konsulenter eller tjenester fra en leverandør, bør man så tidlig som mulig vurdere hvilke verdier disse potensielt vil få tilgang til, og hvilken sikkerhetsrisiko dette kan innebære. Den ansvarlige for anskaffelsen bør sørge for at ansatte med sikkerhetskompetanse også involveres i prosessen.

Når leverandøren eller konsulenten er valgt, bør avtalen inneholde sikkerhetskravene de skal følge. En dialog i forkant vil kunne bekrefte om oppdraget og sikkerhetskravene er forstått. Virksomheten bør følge opp leverandøren eller konsulentselskapet sikkerhetsmessig gjennom hele oppdraget.

Dersom anskaffelsen innebærer tilgang til gradert informasjon, skal sikkerhetslovens krav til graderte anskaffelser legges til grunn.

Husk at en lang kjede av leverandører vil gjøre kontrollen vanskeligere, slik at antall ledd i kjeden bør begrenses i størst mulig grad.

Ved avslutning av oppdraget bør virksomheten ha en avsluttende dialog om hvordan leverandøren eller konsulenten nå skal forholde seg sikkerhetsmessig til informasjonen og kunnskapen den har tilegnet seg. Se for øvrig kapitlet om avslutning av et arbeidsforhold.

7 Juridiske rammer

Flere lover regulerer eller påvirker forholdet mellom arbeidstaker og arbeidsgiver. Enkelte lover er rettet mot spesifikke sektorer, mens andre gjelder for alle. Arbeidsmiljøloven, tjenestemannsloven, likestillingsloven, diskrimineringsloven og personopplysningsloven er viktige lovverk for denne veilederens tema. Her finnes det regler for både hvilke tiltak som kan iverksettes, hva man kan undersøke/spørre om, og hvordan informasjonen skal behandles, lagres og benyttes.

Merk at lov om forebyggende sikkerhetstjeneste regulerer forvaltningsorganer og andre rettssubjekter hvis virksomhet berører forhold knyttet til rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

I en ansettelsesprosess har arbeidsgiver som hovedregel ikke anledning til å innhente opplysninger om jobbsøkers helse, medlemskap i fagforening, samlivsform, seksuell orientering, graviditet, adopsjon, familieplanlegging og standpunkt i kulturelle, politiske og religiøse spørsmål. Unntak gjelder hvis opplysningene er relevante for å vurdere om personen er kvalifisert for stillingen, altså at behovet for opplysningene kan begrunnes i stillingens karakter. Formålet med innhentingen må da beskrives. Siden behandling av personopplysninger skal være basert på et frivillig, uttrykkelig og informert samtykke, må det opplyses om dette så tidlig som mulig, også i utlysningsteksten.

7.1 Personvern

Den enkeltes personvern er en grunnleggende verdi i en demokratisk rettsstat som Norge. Personvernet innebærer at alle har rett til å bestemme over egne personopplysninger og rett til et privatliv. Digitaliseringen av samfunnet kan komme i konflikt med personvernet på flere måter, siden vi stadig får større muligheter for å søke opp andre personers interesser, handlinger og meninger.

Virksomheten må være sikker på at informasjonen den innhenter, er i samsvar med kravene i personopplysningsloven. Loven stiller krav om hjemmel for innhenting av informasjon, formålsavgrensning på bruk av informasjon, samt en rekke krav til behandling og sikring av informasjon.

På Datatilsynets sider finner du god veiledning om personvern (www.datatilsynet.no).

7.2 Politiattest

En politiattest (vandelsattest) inneholder opplysninger om en persons oppføringer i politiregistrene. Det kreves politiattest i flere yrker, og også i en del verv i frivillige organisasjoner. Arbeidsgivere kan bare kreve politiattest fra søkere til en stilling når det står uttrykkelig i en lov eller forskrift at de har anledning til det. Eksempler på slike arbeidsgivere er vaktselskaper, Posten, skoler og barnehager. Det bør gå frem av stillingsutlysningen at politiattest kreves.

Opplysningene i politiets registre er taushetsbelagte. Kun dersom det er hjemlet unntak fra taushetsplikten i politiregisterloven, kan opplysninger deles med andre, herunder andre offentlige og private aktører.

Også i yrker der politiattest ikke er hjemlet i en særlov, kan man møte krav om politiattest. Dette er beskrevet i politiregisterforskriften.

I en ansettelsesprosess er politiattesten bare én, ofte ufullstendig, kilde for å vurdere om en person er egnet for en bestemt stilling. En politiattest og en uttømmende politiattest inneholder kun (straffe-) reaksjoner.

Du finner mer informasjon om politiattester på www.politi.no og i lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) med forskrifter.

Tenk over:

- Hvilke opplysninger har du som arbeidsgiver behov for?
- Er de saklig begrunnet i stillingens karakter?
- Har du i tilstrekkelig grad informert kandidaten om informasjonsbehovet?
- Har vedkommende samtykket?
- Er rutinene for innhenting av opplysninger dokumentert?
- Oppbevarer og behandler du opplysningene i henhold til regelverk?

Viktige lovverk:

- lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)
- lov om statens tjenestemenn m.m. (tjenestemannsloven)
- lov om likestilling mellom kjønnene (likestillingsloven)
- lov om forbud mot diskriminering på grunn av etnisitet, religion og livssyn (diskrimineringsloven om etnisitet)
- lov om behandling av personopplysninger (personopplysningsloven)

Forebyggende sikkerhet:	Tiltak som skal hindre eller redusere effekten av uønskede handlinger. Disse gjennomføres før en uønsket handling finner sted, ideelt for å unngå handlingen i utgangspunktet. Dette er både menneskelige, teknologiske og organisatoriske tiltak.
Personellsikkerhet:	Forebyggende sikkerhetstiltak overfor potensielle ansatte og/eller ansatte for å redusere risikoen for uønsket atferd som truer sikkerheten.
Sårbarhet:	Forhold ved en person som kan medvirke til at han handler i strid med virksomhetens interesser, enten fordi andre utnytter dem, eller fordi de gir personen motivasjon til å utføre slike handlinger.
Trusselaktør:	En aktør som ønsker å utføre en handling eller påvirke andre på en måte som er i strid med norske sikkerhetsinteresser eller en bestemt virksomhets interesser.
Innsider:	En nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.
Verdivurdering:	En analyse som har til hensikt å identifisere hvilke objekter og hvilken type informasjon som utgjør en verdi, hva denne verdien er, og hvilke sikkerhetstiltak som kan beskytte verdien.
Sikringstiltak:	All planlegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av forberedelse til, forsøk på eller gjennomføring av spionasje, sabotasje eller terrorhandlinger.
Bakgrunnssjekk:	Verifisering og/eller innhenting av opplysninger i forbindelse med et ansettelsesforhold.

Publisert:
Mai 2017

Trykk:
Kripos

Layout og illustrasjoner:
Næringslivets Sikkerhetsråd

Foto:
Adobe Stock/Arne Røed Simonsen

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

Adresse:
Middelthuns gate 27, Majorstuen

Mot kriminalitet - for næringsliv og samfunn