Norsk Standard

NS 5835:2024

Publisert: 2024-06-06

Språk: Norsk

Samfunnssikkerhet
Beskyttelse mot tilsiktede uønskede handlinger
Krav til beskyttelse av informasjon og andre verdier i bygge- og anleggsprosjekter

Societal security
Protection against intentional undesirable actions
Requirements for protection of information and other assets in building- and construction projects

Referansenummer:
NS 5835:2024 (no)

Standard Norge

Publiseringsinformasjon

Ved eventuell uoverensstemmelse mellom forskjellige formater, vil PDF-versjon legges til grunn.

ICS: 13.310, 91.020, 91.120.01

Innhold Side

Forord

NS 5835:2024 ble fastsatt 2024-06-06.

Dette dokumentet er utarbeidet av en arbeidsgruppe som utgår fra Standard Norges komité 296 *Samfunnssikkerhet i BAE-sektoren.*

SN/K 296 har medlemmer fra følgende virksomheter:

Advansia

Arkitektbedriftene i Norge

BDO AS

COWI AS

DAVANTI AS

Defendable AS

Departementenes sikkerhets- og serviceorganisasjon (DSS)

Experis AS

Equinor ASA

Forsvarsbygg

F24 Nordics AS

Hansen Security Risk Consulting

Havindustritilsynet

Heiberg & Tveter AS

HRP AS

IFE Holding AS

Kystverket

Multiconsult Norge AS

Norges Bank

Næringslivets Sikkerhetsråd (NSR)

Oslo kommune, Beredskapsetaten

Oslo kommune, Bymiljøetaten

Oslo kommune, MUNCH

Politidirektoratet

Politiets Fellestjenester (PFT)

Proactima AS

Proakt AS

Safetec Nordic AS

Semac AS

Statsbygg

Stortinget

Telenor ASA

Transportøkonomisk institutt (TØI)

Utlendingsdirektoratet (UDI)

Orientering

I alle steg av bygge- og anleggsprosjekter er det nødvendig å håndtere verdier som er beskyttelsesverdige (heretter omtalt som verdier). Dette kan være verdier som eierne av verdiene mener er verdt å beskytte, men hvor det er nødvendig å dele informasjon med aktørene i prosjektet for at tiltaket skal kunne gjennomføres. Med dette risikerer eierne at verdiene blir sårbare. Ved å følge en strategi og en plan for rutiner og prosedyrer kan denne sårbarheten reduseres.

Denne standarden er rettet mot eierne av verdiene i slike prosjekter og er til hjelp for dem som har fått i oppdrag å sikre verdiene som et bygge- og anleggsprosjekt kan få ansvar for å forvalte eller håndtere.

Dette dokumentet bør leses i sammenheng med disse standardene:

— NS 5830:2012 [1], *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Terminologi*;

— NS 5831:2014 [2], *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Krav til sikringsrisikostyring*;

— NS 5832:2014, *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Krav til sikringsrisikoanalyse*;

— NS 5834:2016 [3], *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Planlegging av sikringstiltak i bygg, anlegg og eiendom.*

Dette dokumentet gir et metodisk underlag for å etablere planer og prosedyrer for forebyggende sikringstiltak av alle typer verdier som håndteres i bygge- og anleggsprosjekter, og som eierne er pålagt å beskytte eller mener er verdt å beskytte.

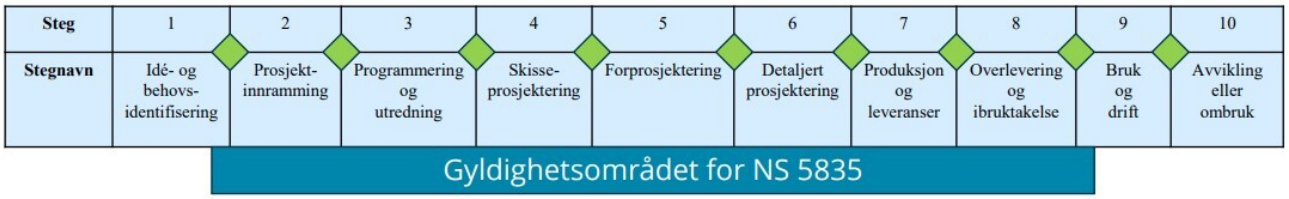
Dokumentet er delt inn i punkter som beskriver aktiviteter for å sikre verdier. I tillegg til den normative hoveddelen har dokumentet seks informative tillegg. Tilleggene har som hensikt å gi praktisk veiledning til bruken og gjennomføring av kravene i hoveddelen og nærmere beskrivelse av gjennomføringen.

Mange av verdiene som skal håndteres, kan være underlagt lover og forskrifter eller andre typer kravdokumenter. Imidlertid finnes det en rekke verdier som ikke omfattes av lover eller forskrifter. Det kan likevel være viktig å beskytte dem av andre årsaker. I slike tilfeller er det viktig at det finnes ett felles system, basert på dette dokumentet, for å ivareta sikringen av verdiene.

I lovverket er det spesielt sikkerhetsloven [4] som kan være relevant for virkeområdet for dette dokumentet.

Dersom verdiene i et bygge- og anleggsprosjekt omfattes av lovverket, gir lovverket sjelden føringer for *hvordan* verdiene skal sikres. Dette dokumentet gir informasjon om mulige tiltaksområder for å sikre verdiene.

Dokumentets gyldighetsområde er fra og med prosjektet begynner å få behov for informasjon og produkter som kan være beskyttelsesverdig, helt til verdiene er sikret og tilbakeført til eieren av verdiene. Dette tilsvarer steg 1–9 i NS 3467 [5], fra steg 1, Idé- og behovsidentifisering, til og med et stykke inn i steg 9, Bruk og drift. Se figur 1.



Figur 1 — Dokumentets gyldighetsområde

Dette dokumentet retter seg hovedsakelig mot fagområdet «sikring» eller «security». Ordene «security» og «safety» er engelske låneord som brukes for å skille mellom sikkerhet mot utilsiktede uønskede hendelser eller ulykker («safety») og tilsiktede uønskede handlinger («security»). Sikkerhet mot tilsiktede uønskede handlinger (security, for eksempel kriminalitet, spionasje og sabotasje) er ut fra NS 5830 [1] omtalt som sikring. Sikring er en handling som utføres for å skape beskyttelse mot en aktør med en tilsiktet uønsket intensjon overfor en entitet. Sikkerhet er vern mot uønskede og utilsiktede hendelser.

I dette dokumentet benyttes sikring enten alene eller sammensatt i de tilfellene der det peker direkte på sikring av en verdi og benyttes sammensatt, for eksempel sikringstiltak, sikringsarbeid, sikringsmål, sikringsrisiko osv. Der begrepene har en sammensatt, større og mer overordnet betydning, benyttes sikkerhet, for eksempel samfunnssikkerhet, sikkerhetsavtale, sikkerhetsplan, sikkerhetsleder osv.

Litteraturlisten angir standarder, normer, lover, forskrifter og annen litteratur som kan være relevant i forbindelse med bruken av dette dokumentet.

Normativ tekst inneholder dokumentets krav. Informativ tekst er kun veiledning til leseren. All tekst i forord, orientering og merknader er informativ tekst. Begrepsmerknader i punkt 3 og eventuelle tillegg i dokumentet kan være enten normative eller informative.

Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til beskyttelse av informasjon og andre verdier i bygge- og anleggsprosjekter

1 Omfang

Dette dokumentet angir rammeverk, krav og retningslinjer for å identifisere verdier som har behov for beskyttelse gjennom forebyggende sikring i bygge- og anleggsprosjekter.

2 Normative referanser

Følgende dokumenter er referert til i teksten på en slik måte at innholdet helt eller delvis inngår som krav i dette dokumentet. For daterte referanser gjelder bare den angitte utgaven. For udaterte referanser gjelder den nyeste utgaven av dokumentet det refereres til (med eventuelle endringer).

NS 5832:2014, *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse*

3 Termer og definisjoner

I dette dokumentet gjelder følgende termer og definisjoner.

3.1
verdi
ressurs som hvis den blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen

[KILDE: NS 5830 [1], 2.18]

3.2
autorisasjon
bekreftelse på at en person eller virksomhet er skikket til å håndtere, og til å bli gitt tilgang til, relevante *verdier* (3.1) i prosjektet

3.3
prosjektsteg
avgrenset stadium i et prosjekt

Begrepsmerknad 1: Prosjektsteg kan igjen være inndelt i delprosesser. NS 3467:2023 [5] definerer stegene i et byggeprosjekt.

[KILDE: NS 3467:2023 [5]]

3.4
oppdragsgiver
person eller foretak prosjektet initieres av

Begrepsmerknad 1: Oppdragsgiver kan tilsvare det plan- og bygningsloven omtaler som «tiltakshaver», eller det NS 8405 [6] og NS 3467 [5] omtaler som «byggherre».

[KILDE: NS 5834:2016 [3], 3.16]

3.5
leverandør
person eller firma som leverer varer og tjenester til prosjektet

Begrepsmerknad 1: Som regel er leverandøren underlagt entreprenøren, men dette bestemmes av gjennomføringsmodellen for det enkelte prosjektet. Spesielle leveranser kan være forankret høyere opp i prosjektets organisering.

[KILDE: NS 5834:2016 [3], 3.19]

3.6
interessent
person, gruppe eller organisasjon som kan påvirke, vil bli påvirket av eller oppfatter at de vil bli påvirket av prosjektets gjennomføring eller resultater

Begrepsmerknad 1: *Aktører* (3.7) er også interessenter.

[KILDE: NS 3467:2023 [5], 3.10]

3.7
aktør
ansvarlig enhet som har en rolle i byggeprosessen

EKSEMPEL Eksempler på en aktør kan være eier, investor, byggherre, arkitekt, rådgiver, produsent, tjenesteleverandør, montasjefirma, utstyrsutleiefirma eller entreprenør.

[KILDE: NS 3467:2023, 3.1 [5]]

3.8
prosjekstsikkerhetsleder (PSL)
ansvarlig for sikkerhetsstyring i bygge- eller anleggsprosjektet

[KILDE: NS 5834:2016 [3], punkt A.6]

3.9
sikringsrisiko
uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen

[KILDE: NS 5832:2014, 3.5]

4 Risikovurdering

Det skal gjennomføres en risikovurdering for å identifisere verdier og å avdekke om disse verdiene kan være utsatt for sikringsrisiko i bygge- og anleggsprosjektet. Dette gjelder for aktører i prosjektet.

I risikovurderingen skal følgende identifiseres:

— hvilke verdier bygge- og anleggsprosjektet har fått til håndtering;

— hvilke trusler verdiene kan bli utsatt for;

— hvilke konsekvenser eksponering for truslene kan ha for verdiene;

— hvilke sårbarheter og mangler som kan identifiseres i eventuelle eksisterende sikringstiltak;

— hvilke tiltak som kan iverksettes for å redusere sårbarheten.

Dette gjelder både for uønskede tilsiktede handlinger og uønskede hendelser.

En risikovurdering bør ledes slik at prosessen bringes effektivt videre fra steg til steg. Den som leder en slik prosess, skal ha kunnskap og kompetanse til å skille mellom begrepene og stegene i prosessen. Risikovurderingen skal brukes som grunnlag for anbefalinger om sikringstiltak som videreføres blant annet i prosjektets sikringsplan.

Risikovurderingen skal utføres som en kvalitativ analyse i henhold til NS 5832:2014.

Se tillegg A for veiledning om risikovurdering.

5 Plan og dokumentasjon

5.1 Prosjektets sikringsplan

En sikringsplan i prosjektet er et styringsdokument for gjennomføring av forebyggende sikring. Sikringsplanen skal utarbeides av oppdragsgiveren basert på anbefalingene fra risikovurderingen og legges til grunn som del av dokumentunderlaget ved utlysninger, kontraheringer og kontrakter i prosjektet. Prosjektets sikringsplan beskriver prosedyrer og bakgrunnsinformasjon vedrørende sikring i prosjektet som er ment for alle involverte aktører.

Sikringsplanen baseres på kjente premisser ved prosjektets begynnelse og etableres så tidlig som mulig i prosjektet. Planen rettes mot alle aktører i prosjektet og bør formuleres på en slik måte at den forstås også av aktører som til vanlig ikke arbeider med beskyttelsesverdig informasjon. Derfor bør planen være så detaljert og konkret som mulig. Det kan være hensiktsmessig å kanalisere deler av prosjektets sikringsplan til definerte steg, slik tillegg C angir.

Prosjektets sikringsplan er ikke et dynamisk dokument, selv om utvikling og endringer i forutsetninger for prosjektet kan medføre behov for endringer i den. Slike endringer bør i så fall dokumenteres tydelig i dokumentet og gjøres kjent for alle som påvirkes av planen. Endringer i dokumentet kan medføre kostnadsendringer. For å forebygge dette, skal dokumentet slik at det gir grunnlag for krav og tiltak med så stor fleksibilitet som mulig, samtidig som krav og ansvar defineres med størst mulig nøyaktighet.

Sikringsplanen skal fastlegges før oppdragsgiveren kontraherer de første leverandørene. Den skal fungere som et sett med prosedyrer rettet mot alle aktørene i prosjektet og legges til grunn for avtaler (se 5.3). Eventuelle senere endringer i prosjektets sikringsplan skal forelegges involverte interessenter.

Prosjektets sikringsplan skal identifisere og definere følgende i alle prosjektets steg, som vist i tabell B.1:

— prinsipper og sikringsmål;

— ansvarsoversikt i prosjektet;

— prosjektets begrensning i tid og omfang;

— relevante lover og regler;

— sikkerhetsprosedyrer;

— forebyggende sikringstiltak;

— beskyttelsesverdige anskaffelser;

— hendelseshåndtering;

— tillatelser, sikkerhetsklareringer og autorisasjon;

— kontroll og revisjon;

— innhold i sikkerhetsavtaler.

Se tillegg B for veiledning om prosjektets sikringsplan.

5.2 Prosjektorganisering for ivaretakelse av sikring

Det skal utarbeides en plan som inkluderer fordeling av ansvar for og oppgaver med sikring av prosjektet under hele prosjektets forløp. Planen skal definere og plassere ansvar og beskrive oppgaver. Dersom oppfølging av sikringen fordeles på flere parter og personer, skal planen vise ansvars- og rollefordelingen mellom disse.

Oppdragsgiveren skal ivareta en koordinerende rolle mot aktørene.

Se tillegg C angir. for veiledning om prosjektorganisering for sikring.

5.3 Sikkerhetsavtaler

Se tillegg D for veiledning om sikkerhetsavtaler.

5.3.1 Generelt

Alle aktører som får kjennskap til eller kommer i kontakt med verdier, skal inngå en sikkerhetsavtale knyttet til prosjektet. Avtalen skal sikre at aktørene pålegges å etterleve prosedyrer og ivareta ansvar for sikring av verdier i prosjektet.

Aktørenes bruk av skytjenester eller andre tjenester som gjør informasjonen sårbar for uønsket eksponering overfor tredjeparter, skal avtales spesielt med den som eier verdien. Dersom den som eier verdien, har krav til hvordan den skal oppbevares, skal dette nedfelles i sikkerhetsavtalen.

MERKNAD Det stilles spesielle krav til sikkerhetsavtaler for prosjekter som er omfattet av sikkerhetsloven (jf. sikkerhetsloven [4] §§ 8-2 og 9-2).

5.3.2 Retur og sletting

Sikkerhetsavtaler i prosjektet skal inneholde krav om at dokumenter og verdier som har blitt overlevert, skal returneres, slettes eller destrueres.

Ved anskaffelsens slutt skal oppdragsgiveren trekke tilbake all beskyttelsesverdig informasjon fra leverandøren og verifisere at den er slettet. Reklamasjonsperioden og eventuell service- og garantitid regnes også som del av anskaffelsen.

5.3.3 Gjennomføring av sikringstiltak hos leverandøren

Leverandørens ansvar for alle beskyttelsesverdige anskaffelser omfatter ansvaret for forebyggende sikring. Mangler som leverandøren selv ikke kan rette på, skal straks rapporteres til oppdragsgiveren. Leverandøren skal også rapportere om sikkerhetstruende hendelser og om forhold som reiser tvil om den sikkerhetsmessige skikketheten til enhver som har befatning med den beskyttelsesverdige anskaffelsen.

Personer som kan få tilgang til beskyttelsesverdig informasjon i prosjektet, skal autoriseres. Leverandøren skal fremme anmodninger om autorisasjon.

Leverandøren skal rette seg etter øvrige gjeldende bestemmelser om sikkerhetsadministrasjon, personellsikkerhet, informasjonssikkerhet og objektsikkerhet.

5.4 Taushetserklæring

Samtlige som får innsyn i og kunnskap om prosjektets verdier, skal avkreves taushetsplikt. Taushetsplikten skal avtalefestes i en signert taushetserklæring. Taushetserklæringen skal signeres av personen som underlegges taushet, og en representant for oppdragsgiveren. Det er normalt prosjektsikkerhetslederen som har oppgaven med å innhente taushetserklæring i prosjektet. Dersom det ikke finnes en dedikert prosjektsikkerhetsleder i prosjektet, skal arbeidsoppgaven ivaretas av oppdragsgiveren.

5.5 Anskaffelser i prosjektet

Anskaffelser med behov for skjerming skal underlegges spesielle prosedyrer for å ivareta informasjonssikkerheten, som skal beskrives i prosjektets sikringsplan (se 5.1). Leveransesikkerheten skal inkluderes i avtaler med leverandører i prosjektet. Slike prosedyrer som ivaretar krav til skjerming, vil berøre tilbudsinnhenting, leveranser til prosjektet og anskaffelsesavtaler og vil legge krav og føringer for hvordan leverandøren behandler bestillinger. Den av prosjekteiers [6] eller leverandørens organisasjon som foretar en anskaffelse eller kjøper en tjeneste som berører sikringen i prosjektet, er ansvarlig for at leverandøren av varen eller tjenesten er gjort kjent med sikringskravene og har de nødvendige autorisasjonene.

6 Kontroll og revisjon

6.1 Virksomhetskontroll

Det skal foretas bakgrunnssjekk av alle virksomheter som skal gis adgang eller tilgang til verdier i prosjektet.

Dersom det er sannsynlig at en kontraktsfestet leverandør blir insolvent i nær fremtid, eller dersom det blir åpnet gjeldsforhandling, skal leverandøren uten ugrunnet opphold informere oppdragsgiveren og holde denne løpende orientert om utviklingen.

6.2 Utlegg, gjeldsforhandlinger eller konkurs hos leverandøren

Utlegg, gjeldsforhandling og konkurs hos leverandører til prosjektet kan føre til uønsket eksponering av beskyttelsesverdig informasjon når leverandøren mister råderetten over sine midler. I prosjektsikkerhetsplanen skal det nedfelles prosedyrer for varsling av boet og at dokumentene bes returnert til prosjekteieren.

MERKNAD 1 Kreditor har rett til dekning i ethvert formuesgode i boet som tilhører debitor på beslagstiden. Imidlertid gjelder ikke dette leverandørens forretningsdokumenter, fordi slike dokumenter ikke lovlig kan omgjøres i penger. Dette gjelder selv om et dokument i særlige tilfeller skulle anses for å ha en økonomisk verdi, f.eks. fordi det inneholder forretningshemmeligheter.

MERKNAD 2 Bobestyrelsens beslagsrett gjelder ikke for dokumenter som leverandøren ikke selv eier, f.eks. dokumenter gradert etter sikkerhetsloven som har blitt utlånt fra prosjektet til leverandøren.

MERKNAD 3 Det kan være verdt å legge merke til at boet kan ha lovlig rett til å tre inn i debitors avtaler, f.eks. leverandørens avtale med prosjektet, og få stilling som kontraktspart. Dette kan i så fall gi bobestyrer og bostyret mulighet for innsyn i dokumenter om sårbarheter og sikringstiltak.

MERKNAD 4 Konkursloven [7] § 80, § 100 første ledd og § 101, samt dekningsloven [8] § 2-1, § 2-2 og § 7-3 første ledd, omhandler problemstillingen med beslag ved gjeldsforhandlinger og konkurs.

6.3 Sikkerhetsrevisjoner

Oppdragsgiveren skal kontrollere sikringsplanen til involverte interessenter i prosjektet og gjøre ettersyn og befaringer av styringssystemene til den enkelte aktør. Dette skal avtales mellom partene på forhånd.

Se tillegg E for veiledning om kontroll og revisjon.

MERKNAD Sikkerhetsloven stiller spesielle krav til kontroll og revisjon for prosjekter som er omfattet av sikkerhetsloven [4] (jf. sikkerhetsloven § 9-2). Forskrift om sikkerhetsgraderte anskaffelser § 2-4 omhandler sikkerhetsmyndighetens samtykke til utlevering og tilvirkning av sikkerhetsgradert informasjon.

7 Personellsikkerhet

7.1 Autorisasjon

Alle som får innsyn og adgang til prosjektets verdier, skal være autorisert.

Det er kun oppdragsgiveren eller den som eier verdien, som kan utstede en slik autorisasjon. Oppgaven med å utstede autorisasjon kan delegeres, men skal da dokumenteres i prosjektets sikringsplan samt i mandatet til den som skal utstede autorisasjonen.

Oppdragsgiveren skal ivareta sikkerheten i prosjektet ved systematisk å vurdere om aktørene i prosjektet er sikkerhetsmessig skikket, og om det bør gjøres endringer i autorisering av personer som er involvert i prosjektet.

Autorisasjonen skal utstedes basert på autorisasjonssamtale, sikkerhetsopplæring og eventuell annen relevant informasjon som viser at vedkommende er sikkerhetsmessig skikket. Taushetserklæring skal foreligge før autorisasjonssamtalen finner sted.

Autorisasjon skal ikke utstedes før bakgrunnssjekk er gjennomført, og er først gyldig når vedkommende har gjennomført sikkerhetsopplæring.

Prosjektets sikringsplan skal beskrive prosedyrer som ivaretar sikringen når autoriserte ansatte fratrer, skifter stilling eller rolle, eller av en annen grunn ikke lenger skal ha tilgang til prosjektets informasjon.

7.2 Adgang, tilgang og innsyn

Oppdragsgiveren har ansvar for å utstede nødvendige autorisasjoner for adgang, tilgang og innsyn i prosjektet.

Leverandøren skal kun gis tilgang til beskyttelsesverdig informasjon dersom det er i samsvar med prosjektets interesser og ikke er i strid med taushetsplikten. Det er oppdragsgiveren som godkjenner leverandører av beskyttelsesverdige anskaffelser.

Disse arbeidsoppgavene kan overføres til andre roller i prosjektet. Slik overføring skal dokumenteres.

7.3 Bakgrunnssjekk

Samtlige personer som involveres i prosjektet, og som får adgang til prosjektets verdier, skal bakgrunnssjekkes.

Se punkt F.2 for veiledning om bakgrunnssjekk.

7.4 Sikkerhetsopplæring

Sikkerhetsopplæringen skal gjennomføres for alle involverte i prosjektet basert på prosjektets sikringsplan. Prosjektsikkerhetslederen skal gjennomføre opplæringen og sikre at ingen tildeles ansvar og autorisasjon før sikkerhetsopplæringen er dokumentert.

Ingen aktør skal få tilganger og autorisasjoner før de har fått instruksjon og signert at de har mottatt og lest informasjon om sikring.

Se tillegg F for veiledning om personellsikkerhet.

Tillegg A
(informativt)

Risikovurdering

A.1 Generelt

En risikovurdering eller -analyse bør foreligge som del av oppstart av et bygge- og anleggsprosjekt og er en forutsetning for å kunne gjennomføre sikkerhetsledelse og et ledelsessystem for sikring i prosjekter. Dette gjelder både for prosjekter med verdier som omfattes av lovverket, og for prosjekter med verdier som faller utenfor lovverkets krav.

Risikovurderinger vil få forskjellig preg avhengig av hva slags bruk og brukere bygningen etableres for.

En risikovurdering bør blant annet peke ut, rangere og vurdere:

— verdier (prioriteres etter hvilke konsekvenser de får ved bortfall eller skade);

— trusler (vurderes ut fra aktuelle interessenter og antatte angrepsmetoder eller hendelser);

— sårbarhet (vurdering av svakheter i eksisterende sikringstiltak);

— mulige tiltak (vurdering av sikkerhetsbehovet og anbefaling av tiltak).

I denne sammenhengen bør risikovurderingen avgrenses til å dekke risiko fra tilsiktede handlinger og utilsiktede hendelser mot verdiene i prosjektet. Risikovurderingen bør omfatte alle steg i et bygge- og anleggsprosjekt.

I det følgende skilles det ikke mellom risikoanalyse og risikovurdering.

A.2 Gjennomføring og deltakelse

Det er oppdragsgiveren som har ansvaret for å gjennomføre en risikovurdering.

En risikovurdering i prosjektet bør foretas av personer med rett kompetanse, og prosessen bør slippe til bred innsikt og ivareta alle hensyn når det involveres deltakere i prosessen, slik at risikovurderingen blir dekkende og fanger opp relevante problemstillinger. I tillegg er det viktig at oppdragsgiveren og ledelsen i virksomheten som eier verdiene, deltar i prosessen.

A.3 Valg av metode

En risikovurdering bør ha grundig dokumentasjon av begrunnelser for og beskrivelse av bakgrunnen for de konklusjonene og anbefalingene som gis.

Det finnes en rekke aksepterte metoder for å gjennomføre risikovurderinger. Gjennomføringsmodell og krav er blant annet beskrevet i NS 5814:2021+AC:2023 [9] og NS 5832:2014.

Så lenge en risikovurdering gjennomføres med deltakelse fra relevante interessenter og gjennomføres med grundig dokumentasjon, kan flere metoder gi akseptable resultater. En god risikovurdering kjennetegnes blant annet ved at den konkluderer med nøye begrunnede anbefalinger av konkrete, målrettede, effektive og målbare risikoreduserende tiltak.

A.4 Verdivurdering

For at en risikovurdering skal bli dekkende, bør interessentene ha en reflektert holdning til hvilke verdier i interessentenes organisasjon som kan bli eksponert og gjort sårbare for uønskede hendelser og handlinger i et bygge- og anleggsprosjekt, enten det dreier seg om materielle eller immaterielle verdier.

Ved prioritering og utpeking av verdier kan det være nyttig å gjennomføre en vurdering av konsekvenser av bortfall eller skade på verdier som blir berørt av prosjektet.

Verdier i prosjekter kan kategoriseres som informasjon, objekter eller infrastruktur.

Verdivurdering bør utføres som første ledd i en risikovurdering.

A.5 Strategi

Det bør beskrives hvilken overordnet strategi som skal benyttes i prosjektet for å håndtere risiko og redusere tap. Strategien angir overordnede grep for å håndtere risiko ved å forebygge risiko, spre risiko, overføre risiko, fjerne verdier eller akseptere risiko.

A.6 Sikringsmål

I verdivurderingen bør det gjøres en vurdering av hva verdiens eier og bygge- og anleggsprosjektet kan akseptere av tap eller skade før det får uønskede eller uakseptable følger for eieren av verdien.

Sikringsmålene setter kriteriene for grunnsikringsnivået i prosjektet i tillegg til de kravene som er pålagt av andre årsaker.

A.7 Trusselvurdering

Som del av en risikovurdering bør handlinger og hendelser som kan true verdiene, vurderes.

— For tilsiktede uønskede handlinger skal mulige trusselaktører, med de handlinger de kan tenkes å ty til for å ramme verdiene, vurderes og prioriteres.

— For utilsiktede hendelser utenfor prosjektet skal mulige ulykker (naturulykker, menneskeskapte situasjoner og tilfeldigheter) vurderes spesielt og prioriteres.

A.8 Sårbarhetsvurdering

Det bør gjøres en vurdering av sårbarheten til de eksisterende sikringstiltakene som vil omgi verdiene i prosjektet i alle steg i prosjektet. Dette skal sees i sammenheng med de truslene som er identifisert i trusselvurderingen.

A.9 Risikoreduserende tiltak

På grunnlag av rangerte verdier, trusler og sårbarheter kan det tas stilling til prioriterte risikoer knyttet til de forskjellige verdiene. Risikoreduserende tiltak anbefales ut fra hvor effektivt de vil redusere risikoen for prosjektets verdier, samtidig som de viktigste punktene i sikringsstrategien følges.

Sikringstiltakene sees i sammenheng med sikringsmålene for å oppnå balansert sikring i prosjektet.

Risikovurderingen legges til grunn for prosjektets sikringsplan.

A.10 Beredskaps- og kontinuitetstiltak

Det bør også etableres en plan for hvilke sikringstiltak som skal iverksettes ved uventet økt risiko, for eksempel ved indikasjon på kriminell aktivitet eller at det uventet blir tilført nye verdier til prosjektet.

Det bør defineres hva bygge- og anleggsprosjektet og eieren av verdien kan akseptere av forstyrrelser og produksjonsavbrudd (kontinuitetsforstyrrelser) før det kan defineres som uakseptabelt. Sikringstiltakene bør som et minimum rette seg etter dette.

Det bør dessuten etableres en plan for tiltak ved sikkerhetstruende hendelser for å vurdere det mulige skadeomfanget og rapportere hendelsen. I slike tilfeller er det også viktig å iverksette tiltak for å avdekke handlingene, sikre bevis, redusere skadeomfanget og hindre gjentakelse.

Tillegg B
(informativt)

Prosjektets sikringsplan

B.1 Generelt

Prosjektets sikringsplan bør koordineres med oppdragsgiverens sikringsplan og eventuelle tilstøtende sikringsplaner og relevante regelverk og rutiner hos oppdragsgiveren eller eieren av verdiene, dersom slikt foreligger.

B.2 Disposisjon

Tabell B.1 viser et eksempel på disposisjon og innhold i en sikringsplan for prosjektet som gjelder for alle steg i prosjektet.

Tabell B.1 — Eksempel på disposisjon og innhold i prosjektets sikringsplan

Tema	Innhold
Prinsipper og sikringsmål	Grunnleggende og overordnede forutsetninger og sikringsmål som ligger til grunn for alle sikringstiltak i prosjektet. Se punkt A.6 for sikringsmål.
Ansvarsoversikt i prosjektet	Overordnet ansvarsmatrise i prosjektet samt roller og ansvar i prosjektet, spesielt når det gjelder sikringen i prosjektet.
Prosjektets begrensning i tid og omfang	Dokumentets gyldighetsperiode (ofte i hele prosjektets varighet). Prosjektets overordnede organisering.
Relevante lover og regler	Relevante lover, forskrifter og andre styrende hjemler og regler som omhandler sikring. Relevante kapitler og paragrafer i lover og forskrifter.
Sikkerhetsprosedyrer	Hvilke deler av prosjektets sikringsrutiner som baserer seg på sikkerhetsprosedyrer fra eierne av verdiene i prosjektet (dersom dette finnes i prosjektet). Prosjektets sikkerhetsrutiner inkludert: — beskrivelse av interessentenes virksomhet og behov for sikring; — prosjektets generelle behov for skjerming (prosjektets generelle graderingsnivå); — oversikt over verdier i prosjektet (kan være typiske dokumenter som tilbudsunderlag, kontrakter eller tegninger eller spesielt maskineri, forsterkninger av bygningen osv.); — hva slags type data i prosjektet som bør beskyttes, og liknende); — presentasjon av hjemler og regler for informasjonsbeskyttelse; — beskrivelse av prosjektets prosedyrer for produksjon, merking og håndtering av beskyttelsesverdig informasjon (journalføring, kopiering, makulering, fotografering, oppbevaring, forsendelse og kontroll); — organisatoriske prosedyrer for å håndtere sikkerhetsmessige anskaffelser.
Forebyggende sikringstiltak	Beskrivelse av grunnsikringstiltak for fysisk sikring av lokaler, byggeplass, adgangskontroll, varsling, dokumenthåndtering osv.
Beskyttelsesverdige anskaffelser	Håndtering av anskaffelser av elementer i prosjektet som krever spesiell beskyttelse, og som representerer en spesiell verdi for prosjektet, oppdragsgiveren eller viktige interessenter.
Hendelseshåndtering	Avdekking, varsling, rapportering, utrykning, skadebegrensning, vurdering av skadeomfang, sikring av bevis og hindring av gjentakelse.

Tabell B.1 — Eksempel på disposisjon og innhold i prosjektets sikringsplan *(fortsetter)*

Tema	Innhold
Tillatelser, sikkerhetsklarering og autorisasjon	Prosedyrer for å søke om og få tillatelser, klareringer og autorisasjoner i prosjektet (for eksempel godkjenning av et informasjonssystem som er skjermingsverdig etter lovverket). Dette gjelder også prosedyrer ved fratreden fra stillinger eller roller med autorisasjon.
Opplæring og informasjon	Ansvarsforhold, metode, gjennomføring og dokumentasjon av sikkerhetsopplæring av aktører i prosjektet. Informasjonsformidling i prosjektet når det gjelder sikring.
Revisjon	Sikkerhetsrevisjon i prosjektet. Kontroll og revisjon av at aktørene i bygge- og anleggsprosjektet etterlever prosjektets sikringsplan.
Innhold i sikkerhetsavtaler	Se 5.3 og informativt tillegg D.

Tillegg C
(informativt)

Organisering, roller og ansvar

C.1 Generelt

Et bygge- og anleggsprosjekt involverer en rekke interessenter og aktører og er organisert hierarkisk. Disse rollene kan variere fra prosjekt til prosjekt avhengig av anskaffelsesstrategien, men følger som regel et generisk mønster. Rollene og grupperingene kan også variere etter prosjektets steg, anskaffelsesstrategi og entrepriseform, og aktører kan skifte rolle og tilhørighet underveis i prosjektet.

Entreprenører blir normalt kontrahert på grunnlag av beskrivelser eller forprosjekter. Når en entreprenør kontraheres inn i et bygge- og anleggsprosjekt, vil antall aktører i byggeprosjektet øke, og prosjektet endrer karakter fra planleggingsmodus til konkret gjennomføringsmodus. Dette innebærer også at sikringen blir mer utfordrende, og da er det ekstra viktig å ha systemer og rutiner på plass for å håndtere det økte antallet aktører.

En totalentreprise, jf. NS 8407 [10], vil medføre at entreprenøren påtar seg ansvaret for planleggingen, og at de prosjekterende blir underlagt entreprenøren, mens de tidligere var underlagt oppdragsgiveren. I en utførelsesentreprise, jf. NS 8405 [6], vil de prosjekterende forbli direkte underlagt oppdragsgiveren og sidestilt med entreprenøren.

Sikring av verdier i et bygge- og anleggsprosjekt forutsetter lederengasjement på alle nivåer. God forankring av ansvaret for oppfølging er avgjørende for måloppnåelse. Det endelige ansvaret for sikringen i bygge- og anleggsprosjekter ligger hos den øverste lederen i prosjektet. Selv om dette ansvaret ikke kan delegeres, kan og bør arbeidsoppgaver for å ivareta sikringen i prosjektet defineres som ansvar hos aktørene i prosjektet. Dersom det blir utpekt en prosjektsikkerhetsleder, er det hensiktsmessig at ansvaret for sikkerhetsstyring ligger hos vedkommende.

C.2 Den enkeltes ansvar

Alle aktørene i prosjektet bør holdes ansvarlig for sine oppgaver, og det bør stilles krav til at alle kjenner til og overholder kravene og prosedyrene for sikring i prosjektet.

Dette forutsetter at alle aktører i prosjektet har fått instruksjonene og informasjonen som er nødvendig for å kunne overholde kravene. Dette bør dokumenteres av nærmeste overordnet i ansvarskjeden.

C.3 Fordeling av ansvar

Oppdragsgiveren bør så langt det er mulig, fordele arbeidsoppgaver knyttet til sikringen til definerte aktører i definerte roller i prosjektet, der hver av rollene har ansvar for sine arbeidsoppgaver. Ivaretakelse og kontroll av sikringen bør samordnes med prosjektets øvrige aktiviteter.

C.4 Spesielle roller

Ved større prosjekter eller anskaffelser som involverer beskyttelsesverdig informasjon, bør det utpekes en prosjektsikkerhetsleder. Tildeling av rollen som prosjektsikkerhetsleder kan være avhengig av prosjektenes entrepriseform og gjennomføringsmodell. I en utførelsesentreprise vil de prosjekterende være kontrahert av byggherren, og da vil en av de prosjekterende kunne bli utpekt som prosjektsikkerhetsleder. I en totalentreprise vil de prosjekterende være engasjert av totalentreprenøren. I dette tilfellet vil det være naturlig at prosjektsikkerhetslederen knyttes direkte til byggherresiden.

Prosjektsikkerhetslederen og utpekte personer i prosjektorganisasjonen bør sørge for koordinering, rådgivning og kontroll av sikringen i alle ledd i prosjekteiers organisasjon. For entreprenøren bør det utpekes en tilsvarende rolle i entreprenørens organisasjon som rapporterer til prosjektsikkerhetslederen.

Det er viktig at prosjektsikkerhetslederen og entreprenørens sikkerhetsleder rapporterer til oppdragsgiveren og eierne av verdiene når det gjelder viktige sikkerhetssaker i prosjektet.

Rollen er også beskrevet i NS 5834:2016 [3], punkt A.6.

C.5 Administrativ sikring gjennom prosjektsteg 2–7

Sikringsorganiseringen i et byggeprosjekt må tilpasses slik at byggearbeidene kan gjennomføres så tids- og kostnadseffektivt som mulig. Samtidig skal verdiene i prosjektet bli ivaretatt på en god måte. Derfor bør ansvaret defineres og plasseres hos aktører som kjenner sin rolle og sitt ansvar, og som har kompetanse til å ivareta dette. På samme måte som NS 5834 [3] angir behov for spesiell kompetanse i prosjekteringen, må også det administrative ansvaret behandles med den kompetansen som er nødvendig. NS 5834 [3] har definert dette i beskrivelsen av en informasjonssikkerhetsplan for prosjektet (B.1.6).

Det går et skille i sikringsorganiseringen i et byggeprosjekt ved overgangen mellom stegene i et prosjekt (3.3).

C.5.1 Steg 2: Prosjektinnramming

Dette steget preges av utredninger og alternativsvurderinger for å definere hvordan prosjektet skal gjennomføres. De forskjellige alternative løsningene utredes, og konsekvensen av disse blir presentert. Som resultat av dette steget tas det en avgjørelse om hvilket løsningsalternativ som skal velges og utvikles videre. I dette prosjektsteget blir det produsert en behovs- og funksjonsanalyse.

Som del av dette steget beskrives de nødvendige prosjektadministrative sikringstiltakene for hvert enkelt alternativ med de konsekvensene de får for f.eks. modell- og tegningshåndtering, datasikkherhetsløsninger, organiseringsprisipper osv. i prosjektet, med blikk for effektiv bruk og forvaltning. Detaljene bør være så klare at det er mulig å gjennomføre en autorisasjonssamtale.

Dette steget involverer flere ekspertaktører som bør klareres og autoriseres inn i prosjektet i henhold til denne standarden.

C.5.2 Steg 3: Programmering og utredning

I dette steget konstateres det om den valgte løsningen er gjennomførbar, og det velges prinsippløsning. Her utarbeides grove kostnadsestimater og nyttevurderinger.

Prosjektsikkerhetsplanen utarbeides her i første utkast basert på de innspillene som blir lagt frem av prosjektadministrativ art for sikringen. Kalkulasjon av konsekvensene av anbefalt prosjektadministrativ løsning for sikringen skal legges frem og inngå som del av vurderingen av om det er grunn til å gå videre med prosjektet. Dette innebærer at det skal foreligge tanker om detaljløsninger og organisering.

Dette steget innebærer flere aktører enn i foregående steg, men prosjektet er foreløpig sparsommelig bemannet av eksterne aktører. Disse bør klareres og autoriseres inn i prosjektet i henhold til denne standarden.

C.5.3 Steg 4: Skisseprosjektering

Dette steget skal bearbeide videre de løsningene som ble valgt som resultat av forrige steg. Her utvikles og realitetsprøves alle tekniske løsninger i prosjektet, og det utvikles et skisseprosjekt med tekniske løsninger og planer for tiltaket for å vurdere iverksetting og finansiering. Enkelte prosjekter kontraherer en entreprenør allerede på dette stadiet.

For intern administrativ sikring i prosjektet innebærer dette stadiet at prosjektsikkerhetsplanen bør få sin endelige form, og aktørene i prosjektet bør forholde seg til denne.

I forbindelse med dette steget vil flere aktører bli involvert, spesielt fra arkitekt og prosjektleder, og flere eksterne aktører vil få innsyn i prosjektet.

C.5.4 Steg 5: Forprosjektering

På dette stadiet utvikles prosjektet fra skissestadium til forprosjekt, der systemvalg og hovedløsninger besluttes. På dette stadiet foreligger det utviklede kostnadsvurderinger i prosjektet.

For intern administrativ sikring i prosjektet innebærer dette at prosjektsikringsplanen stadfestes og legges til grunn for alle kravspesifikasjoner som nå utvikles i prosjektet. På dette stadiet utvikles opplæringsunderlag for leverandører og entreprenører.

På dette stadiet er hele planleggingsteamet på plass.

C.5.5 Steg 6: Detaljert prosjektering

På dette stadiet prosjekteres alle løsninger i prosjektet i detalj for å sikre rett og sikker utførelse med detaljerte tegninger og beskrivelser. Dersom entreprenører allerede er kontrahert, vil detaljprosjekteringen styres eller påvirkes av disse.

For intern administrativ sikring i prosjektet vil dette påvirke gjennomføringsmodellen og måten entreprenøren gjennomfører sine arbeider på, både i rigg og i sin egen administrasjon. Det er viktig at sikringsprosedyrene er tydelig beskrevet i underlagsdokumentasjonen og kontraktsunderlaget. Entreprenøren må forholde seg til prosjektsikkerhetsplanen. Opplæringsunderlaget må på plass som del av de administrative rutinene til entreprenøren.

På dette stadiet er hele planleggingsteamet på plass, og entreprenørens hovedaktører kan også ha gått i gang med arbeidene.

C.5.6 Steg 7: Produksjon og leveranser

Dette er steget der byggearbeidene blir gjennomført. Produksjonen gjennomføres i henhold til planer og avtalte kvaliteter. Dette gjelder også prosedyrer og systemer for administrativ sikring av prosjektet.

Dette er en utfordrende og hektisk periode for prosjektsikkerhetslederen, som har ansvaret for å følge opp at prosjektet blir gjennomført etter hensikten, og for at det foretas opplæring og kursing av alle involverte i byggeprosjektet.

På dette stadiet er prosjektet i full drift, og for utenforstående kan det virke kaotisk. Byggeprosjektet har nådd sin største bemanning.

C.5.7 Steg 8: Overlevering og ibruktakelse

Overlevering av ferdig bygg. I dette steget rettes alle feil, slik at produksjonen kan regnes som ferdig. Entreprenøren rigger ned, og resultatet tas i bruk.

I denne perioden kan det oppstå forsinkelser i leveranser av sikkerhetsutstyr som overvåkingsanlegg, fysiske sikringstiltak osv., som oppdragsgiver ønsker å være spesielt forsiktig med å spre informasjon om.

Så snart prosjektet går over til å være et bygg eller anlegg i daglig drift, forsvinner også behovet for administrativ sikkerhet i prosjektet. All dokumentasjon overlates til en driftsorganisasjon, og nødvendig dokumentasjon overføres til FDV-systemet.

Tillegg D
(informativt)

Sikkerhetsavtaler

D.1 Generelt

Det bør tegnes en sikkerhetsavtale med alle involverte interessenter, som prosjekterende, entreprenører og leverandører i prosjektet. Denne bør minst regulere følgende forhold:

— prosjektets navn og sikkerhetsgradering med vedlagt graderingsspesifikasjon;

— taushetserklæring fra og autorisasjon av personell hos leverandøren som vil kunne få tilgang til prosjektets informasjon;

— utlevering og bekjentgjøring av beskyttelsesverdig informasjon til tredjeparter, herunder til underleverandører, konsulenter, målgrupper for markedsføring og media;

— forvaltning av beskyttelsesverdig informasjon, herunder eventuell godkjenning for bruk av informasjonssystemer og tilbakelevering av maskiner, lagringsmedier osv.;

— omkostninger ved sikkerhetstiltak;

— varslinger om flytting av leverandørens lokaler som påvirker beskyttelse av informasjonsverdier;

— varslinger om endringer i styret, endring av daglig leder og endring av firmanavn med videre;

— varsling ved fratredelse av stilling eller endring av roller og ansettelse av nye ansatte;

— tilbakelevering av informasjonsverdier i prosjektet ved utløp av en eventuell anbudsfrist og ved det sikkerhetsgraderte oppdragets slutt;

— prosedyrer for varsling og tiltak ved insolvens, gjeldsforhandling og konkurs;

— tiltak og konsekvenser ved sikkerhetsbrudd;

— oppdragsgivers rett til sikkerhetsinspeksjon for prosjektansvarlig eller myndigheter;

— spesielle vilkår, ved for eksempel konkurs;

— sikkerhetsavtalens gyldighetstid;

— endringer i sikkerhetsavtalen.

D.2 Gjennomføring av sikkerhetstiltak hos leverandøren

Prosjektadministratoren bør kreve at det foretas sikkerhetsrevisjon hos leverandøren før denne kan bli endelig godkjent, og det bør også føres tilsyn underveis i prosjektet.

D.3 Adgang, tilgang og innsyn

Autorisasjon innebærer normalt en samtale med den som autoriseres, der prosjektets sikringsplan gjennomgås og sikkerhetsavtaler og taushetserklæringer signeres. En slik samtale bør normalt foretas av prosjektlederen eller prosjektsikkehetslederen.

D.4 Entreprenører, leverandører og rådgivere

Prosjektsikkerhetslederen skal føre oversikt over alle aktørene i hele entreprenør-, leverandør- og rådgiverkjeden som er godkjent for leveranser og ytelser til prosjektet, og over de sikkerhetsavtalene som er inngått.

D.5 Personer som slutter

Det bør føres dokumentert kontroll med at personellet leverer inn de av prosjektets beskyttelsesverdige dokumenter de er i besittelse av, og nøkler, adgangskort og annet materiell som gir tilgang til sikkerhetsgradert informasjon. Dersom taushetsplikten også gjelder etter fratreden eller skifte av stilling eller rolle, bør det gjøres oppmerksom på dette. Kontaktinformasjonen til de som slutter, bør oppbevares hos oppdragsgiveren i en bestemt tid etter fratredelse.

Tillegg E
(informativt)

Kontroll og revisjon

E.1 Generelt

Det bør gjennomføres en bakgrunnssjekk av alle virksomheter tilknyttet prosjektet, inkludert rådgivere, entreprenører, leverandører og underentreprenører. Dette inkluderer også små virksomheter. Kontroll av enkeltpersonsforetak kan utføres som bakgrunnssjekk av en person.

Lovverket setter grenser for hva som kan innhentes og kreves levert av den enkelte virksomhet uten samtykke fra den berørte. Skatteattest, angivelse av virksomhetsnummer, tidligere regnskap, firmaattester og referanser, godkjenninger og sertifikater kan leveres av virksomheten selv. Ytterligere kontroll kan gjøres gjennom enhetsregisteret, kredittopplysninger av virksomheter og eiere og kontroll og oppfølging av virksomhetens opplysninger. Virksomhetskontroll bør også innbefatte bakgrunnssjekk av eiere, styreleder og daglig leder.

Mye av denne informasjonen kan innhentes under tilbudsinnhentingen. Det er viktig at informasjonen er oppdatert og oppdateres løpende dersom det skjer endringer i kontraktsperioden.

E.2 Kontroll av virksomhetene i prosjektet

Det vil være forskjellige hjemmelsgrunnlag og behov for de prosjektene som har verdier som er omfattet av lovverket, og prosjekter med verdier som ikke er det. Opplistingen i punkt E.3 og punkt E.4 nedenfor skal vurderes av prosjektansvarlig og brukes som grunnlag for krav til alle virksomheter som er tilknyttet prosjektet.

E.3 Vurderingsgrunnlag

Ved vurdering av om virksomheten er skikket til å levere varer eller tjenester til prosjektet, kan følgende opplysninger knyttet til leverandøren vektlegges:

— økonomiske forhold, herunder muligheten for insolvens, eierform og eierinteresser;

— sikkerhetsmessige forhold for daglig leder og styret;

— sikkerhetsorganisasjonen;

— gjennomførte sikkerhetstiltak;

— mulige straffbare forhold, herunder forhold som kvalifiserer til foretaksstraff;

— andre forhold som kan gi grunn til å frykte at leverandøren vil kunne opptre i strid med oppdragsgiverens sikkerhetsmessige interesse.

E.4 Virksomhetskontroll

Virksomheter som leverer varer eller tjenester til prosjektet, bør gi egenopplysninger til prosjektleder og prosjektsikkerhetsleder. Omfanget av opplysningene kan variere, men det anbefales å be om minst følgende opplysninger:

— navn (firma), adresse og eierform;

— om virksomheten er registrert i Brønnøysundregistrene;

— personer i styret og ledelsen med navn og fødselsdato;

— tidligere oppdrag med oppdragsgivere og referanser;

— årsrapporter og årsregnskap;

— skisse/tegninger over de lokalene som er tenkt benyttet av virksomheten til arbeid med tjenesten/leveransen;

— sikkerhetstiltak i de lokalene som er tenkt benyttet til arbeid med tjenesten/leveransen.

Dersom prosjektet er underlagt en eller flere lover som berører sikringen i prosjektet, kan dette legges til i listen ovenfor.

E.5 Prosedyrer ved insolvens og konkurs

En bestemmelse om varsling av aktørers insolvens, gjeldsforhandling eller liknende bør inkluderes i leverandørkontrakten, slik at prosjektansvarlig får tatt de nødvendige forholdsregler før konkursen er en realitet, og det blir tatt beslag i boet.

Det bør kontraktfestes at prosjektansvarlig har rett til å pålegge ekstra sikringstiltak dersom det er grunn til å mistenke fare for konkurs eller insolvens.

For å forebygge slike situasjoner bør det velges leverandører med robust økonomi i alle ledd i en leveranse som berører sikring av verdier. Dette bør annonseres tydelig i utlysninger og tilbudsgrunnlag og gis tilstrekkelig undersøkelse ved tilbudsevaluering.

E.6 Sikkerhetsrevisjon

I forbindelse med utmåling av sikringstiltak og fremsetting av krav til aktørene når det gjelder sikring av verdiene i prosjektet, bør det etableres systemer for å kontrollere at aktørene etterlever kravene. Dette angis i prosjektets sikringsplan.

Tillegg F
(informativt)

Personellsikkerhet

F.1 Generelt

Prosjekter som er omfattet av lovverket, har andre hjemmelsgrunnlag når det gjelder bakgrunnssjekk enn de prosjektene som faller utenfor. Derfor vil bakgrunnssjekk og taushetserklæring variere avhengig av hvilke lover prosjektet er underlagt.

F.2 Bakgrunnssjekk

Vurdering om en person er sikkerhetsmessig skikket, baseres på informasjon fra bakgrunnssjekken og inntrykket fra en sikkerhetssamtale. Vurderingen bak beslutningen bør begrunnes og dokumenteres.

Bakgrunnssjekk krever normalt samtykke fra den som kontrolleres. Lovverket regulerer hva som tillates av innhenting av informasjon både med og uten samtykke, og hvordan slik informasjon oppbevares.

Normalt regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted som personsensitive forhold med mindre denne typen informasjon avslører andre beskyttelsesverdige forhold.

For å sikre likebehandling, effektivitet og konfidensialitet for bakgrunnssjekker bør én aktør, fortrinnsvis prosjektsikkerhetslederen, gis oppgaven å gjennomføre bakgrunnssjekken. Personen som bakgrunnssjekkes, bør gis informasjon om hvordan denne prosessen vil foregå, at det vil bli gjennomført en bakgrunnssjekk, og konsekvensene av å oppgi feilaktige opplysninger.

Det bør kreves at vedkommende som skal bakgrunnssjekkes, oppgir minst:

— fullt navn, inkludert tidligere navn hvis aktuelt;

— fødselsdato og -år;

— nåværende og tidligere adresser med dato og årstall;

— utdannings- og ansettelseshistorikk med dato og årstall;

— utfyllende opplysninger fra kandidaten.

Disse opplysningene bør gis i et eget skjema der personen gir et skriftlig signert samtykke til at det hentes inn informasjon fra for eksempel tidligere arbeidsgivere, kredittinstitusjoner [5] og andre. Regler for dette er gitt i personopplysningsloven [11]. Et samtykkeskjema bør minst inneholde følgende informasjon til den som skal kontrolleres:

— 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;

— henvisning til personopplysningsloven og rettighetene til den som skal bakgrunnssjekkes;

— hvor, hvor lenge og hvordan opplysningene skal oppbevares, med henvisning til relevante lover og forordninger.

Det bør angis hvordan avslag til samtykke fra den kontrollerte personen kan bli tolket og behandlet.

En bakgrunnssjekk kan deles inn i fem hoveddeler:

— identitetskontroll og verifikasjon;

— verifisering av informasjon (familieforhold, autorisasjoner, godkjenninger og tillatelser);

— eventuell kontroll av gyldig opphold;

— kredittsjekk og sjekk av næringsinteresser;

— søk i åpne kilder.

F.3 Sikkerhetsorientering

Alle personer som er ment å få autorisasjon og tilganger i prosjektet, bør få sikkerhetsopplæring. Slik opplæring kan gis i grupper, gjerne som del av møter, og foretas på grunnlag av prosjektets sikringsplan.

Dokumentasjon av sikkerhetsopplæring bør gjøres skriftlig og oversendes prosjektsikkerhetsleder eller prosjektleder. Dokumentasjonen kan etableres som del av møtereferat eller som melding. Det kan etableres et system for signering av gjennomført opplæring og mottatt og lest informasjon.

F.4 Taushetserklæring

I prosjekter som ikke håndterer verdier som er underlagt lovverket, er det ikke anledning til å stille samme krav som i prosjekter som håndterer verdier som er underlagt loven. Hjemmel for taushetserklæringen bør alltid angis.

MERKNAD 1 Prosjekter som er underlagt sikkerhetsloven, følger egne lovpålagte prosedyrer.

Følgende eksempel på taushetserklæring kan benyttes for prosjekter som ikke er underlagt sikkerhetsloven:

EKSEMPEL Undertegnede, som har oppgaver i prosjektet [prosjektets navn] (heretter kalt prosjektet), forstår at jeg i forbindelse med mitt arbeid kan få kjennskap til forhold av betydning for oppdragsgiver og prosjektets involverte interessenter. Dette kan være beskyttelsesverdige opplysninger som gjelder beskyttelse eller sårbarhet, tekniske innretninger, opplysninger om drifts- eller forretningsforhold, opplysninger av konkurransemessig betydning eller opplysninger som skal sikres konfidensialitet av andre grunner.

Jeg forplikter meg til ikke å omtale, bruke, vise, utlevere eller på annen måte tilgjengeliggjøre informasjon overfor uvedkommende som jeg skriftlig, muntlig, elektronisk eller på annen måte får kjennskap til gjennom prosjektet. Taushetsplikten gjelder også overfor andre i prosjektet som ikke har behov for vedkommende informasjon i sitt arbeid. Som uvedkommende regnes også ansatte i min egen virksomhet i prosjektorganisasjonen som ikke har funksjonelle behov for vedkommende informasjon i sitt arbeid.

Jeg forplikter meg også til å utvise spesiell aktsomhet når det gjelder tilbudsevaluering, prosjektspesifikasjoner, tekniske og andre beregninger, beskrivelser, modeller, kontrakter eller lignende.

Taushetsplikten gjelder også for informasjon om oppdragsgivere og forretningsforbindelser og andre forhold jeg blir kjent med gjennom prosjektet.

Ved avslutning av mitt oppdrag for prosjektet plikter jeg å tilbakelevere eller dokumentere at jeg har tilintetgjort all beskyttelsesverdig dokumentasjon i prosjektet (både fysisk og elektronisk) som jeg måtte være i besittelse av, og som jeg har mottatt gjennom prosjektet.

Jeg godtar denne taushetsplikten både i perioden jeg er engasjert i prosjektet, og etter at oppdraget for prosjektet er avsluttet.

Jeg er klar over at taushetsplikten gjelder både i og utenfor tjenesten, også etter endt arbeidsforhold.

Jeg bekrefter at jeg har satt meg inn i lovverket ...

(Opplisting av relevante lover med hjemler og paragrafer. Listen bør være veiledende ut fra hvilke lover og paragrafer som regulerer taushetsplikten.)

Brudd på denne taushetserklæringen vil medføre straffeansvar etter straffeloven og (relevante lovmessige konsekvenser angis, for eksempel som gitt i markedsføringsloven). Videre vil overtredelse kunne innebære erstatningsansvar etter (erstatningsansvar etter lovverket angis, for eksempel som gitt i aksjeloven § 17-1).

Denne erklæringen er utferdiget i to eksemplarer, hvorav prosjektansvarlig og undertegnede beholder hvert sitt. Den sist daterte underskrevne taushetserklæringen gjelder. Eventuelle tidligere underskrevne taushetserklæringer utgår.

Sted og dato:

Signatur av person underlagt taushetsplikt og prosjektsikkerhetsleder

MERKNAD 2 Sikkerhetsloven krever at virksomheter og personer som skal ha tilgang til skjermingsverdig informasjon, er klarert gjennom en klareringsmyndighet, og stiller spesielle krav til personellsikkerhet i lovens kapittel 8 og virksomhetsikkerhetsforskriftens kapittel 12 [12]. For slike prosjekter benyttes statens taushetserklæring med referanse til sikkerhetsloven.

Litteratur

[1] NS 5830:2012, *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Terminologi*

[2] NS 5831:2014, *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Krav til sikringsrisikostyring*

[3] NS 5834:2016, *Samfunnssikkerhet — Beskyttelse mot tilsiktede uønskede handlinger — Planlegging av sikringstiltak i bygg, anlegg og eiendom*

[4] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)

[5] NS 3467:2023, *Steg og leveranser i byggverkets livsløp*

[6] NS 8405:2008, *Norsk bygge- og anleggskontrakt*

[7] Lov 8. juni 1984 nr. 58 om gjeldsforhandling og konkurs (konkursloven)

[8] Lov 8. juni 1984 nr. 59 om fordringshavernes dekningsrett (dekningsloven)

[9] NS 5814:2021+AC:2023, *Krav til risikovurderinger*

[10] NS 8407:2021, *Alminnelige kontraktsbestemmelser for totalentrepriser*

[11] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

[12] Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)

- Norsk Standard fastsettes av Standard Norge og er varemerkebeskyttet.
- Andre leveranser fra Standard Norge, som tekniske spesifikasjoner, workshopavtaler og veiledninger, utgis etter ferdigstilling uten formell fastsetting.
- Standard Norge kan gi opplysninger om innholdet og svare på faglige spørsmål.
- Spørsmål om gjengivelse rettes til Standard Online AS.
- Inntektene fra salg av standarder utgjør en stor og avgjørende del av finansieringen av standardiseringsarbeidet i Norge.
- Mer informasjon om standardisering, standarder, kurs og andre produkter finnes på *www.standard.no*.

Standard Norge
Postboks 242
1326 Lysaker
Telefon 67 83 86 00
info@standard.no

www.standard.no

Standard Online AS
Postboks 242
1326 Lysaker
Telefon 67 83 87 00
salg@standard.no

Referansenummer:
NS 5835:2024 (no)

Standard Norge