Nasjonal sikkerhetsmyndighet

Veiledning

Sist oppdatert: 2015-04-08

Fysisk sikring mot ulovlig inntrengning

Veiledning til forskrift om informasjonssikkerhet

Forskrift om informasjonssikkerhet stiller krav til forebyggende sikkerhetstiltak mot ulovlig inntrengning. Bestemmelsene gjelder generelt for alle virksomheter som faller inn under sikkerhetslovens virkeområde og er å anse som minimumskrav til sikringstiltak i en normalsituasjon. Forskriften gir i noe utstrekning anledning til å kompensere for tiltak som ikke kan oppfylles, og den pålegger NSM å stille krav og forestå ulike godkjenninger.

Denne veilederen utdyper forskriftens bestemmelser, orienterer om NSMs gjeldende godkjenninger, samt gir råd om alternative kompenserende sikringstiltak. Veilederen er ikke ment å kun brukes separat, men forutsetter kunnskap om forskriftens innhold og må ses sammen med de konkrete krav som denne stiller.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20 mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internettadresse
www.nsm.stat.no

Innhold

1 Innledning 4
2 Generelt om behandling og oppbevaring av sikkerhetsgradert informasjon 4
3 Inndeling og sikring av fysiske områder 5
3.1 Definisjon av de enkelte områder 5
3.2 Kontroll med adgangen til de enkelte områder 6
3.2.1 Kontrollert område 6
3.2.2 Beskyttet område 6
3.2.3 Sperret område 7
3.3 Sikring av de enkelte områder 7
3.3.1 Kontrollert område 7
3.3.2 Beskyttet område 8
3.3.3 Sperret område 8
3.3.4 Tilsyn 10
4 Oppbevaringsenheter for sikkerhetsgradert informasjon 10
4.1 Oppbevaringsenheter for BEGRENSET 10
4.2 Oppbevaringsenheter for KONFIDENSIELT 11
4.3 Oppbevaringsenheter for HEMMELIG 12
4.4 Oppbevaringsenheter for STRENGT HEMMELIG 12
5 Sikring av informasjonssystemer, kabelsystemer og nettverkskomponenter 13
5.1 Kabler 13
5.2 Kummer 13
5.3 Nettverkskomponenter 13
5.4 Servere 14
5.5 Brukerterminaler/kontorer 14
5.6 Skrivere 14
5.7 Risikovurdering og dokumentasjon 14
6 Håndtering av nøkler og koder 15
6.1 Nøkkelskap 15
7 Låser 16
7.1 Avlåsing generelt 16
7.2 Låser for BEGRENSET 16
7.3 Låser for KONFIDENSIELT 17
7.3.1 Valg av låstype 17
7.3.2 Låskasser 18
7.4 Låser for HEMMELIG / STRENGT HEMMELIG 18
7.4.1 Lås # 1, hovedlås 18
7.4.2 Lås # 2, tilleggslås 19
7.5 Daglås og krav til rømning 19
8 Dører 20
9 Elektronisk sikring 20
9.1 Adgangskontrollsystemer 20
9.1.1 Anskaffelse 21
9.1.2 Automatiske adgangskontrollanlegg for spesialrom 21
9.1.3 Registrering 22
9.2 Innbruddsalarmsystemer 22
9.2.1 Anskaffelse 22
9.2.2 Alarmlegging av særlig viktige rom 23
9.3 Kameraer 23
9.3.1 Anskaffelse 23
9.3.2 Registrering 24
9.4 Bruk av elektroniske sikringsanlegg 24
10 Plombering 24
10.1 Emballasje 24
10.2 Plomberingsutstyr 25
11 Dokumentasjon 25
12 Dokumenthistorie 26
Kontrollskjema for automatiske adgangskontrollanlegg 27
Kontrollskjema for innbruddsalarmanlegg 33

Kontrollskjema for kameraovervåkingsanlegg..... 38

1 Innledning

Det er viktig å merke seg at det ikke finnes sikringsmidler som er helt sikre. Det er ingen fysisk barriere som ikke lar seg forsere, ei heller låser og alarmsystemer som ikke kan manipuleres. Det er kun snakk om tilstrekkelig tid, kunnskap og verktøy. Bruk av ett sikringsmiddel alene gir derfor sjelden noen god løsning. Man kan si at fysiske sikringstiltak i hovedsak tjener tre formål: deteksjon, tidsforsinkelse og reaksjon. Dersom ett sett av disse tiltakene ikke er tilstede avtar effekten av de andre dramatisk. Dersom et innbruddsforsøk ikke fremkaller motreaksjon spiller det mindre rolle hvor lang tid det tar å forsere en barriere – forsøket vil lykkes. Man bør derfor søke å følge prinsippet om sikring i dybden - en kombinert løsning med deteksjonsmuligheter og tidsforsinkende barrierer i flere ledd, samt et reaksjonsapparat med reell evne til å stanse en inntrenger.

Det er også viktig å være klar over at sikkerhet ikke er et fysisk produkt. Massivitet og tekniske finesser gir ikke nødvendigvis god sikring dersom det skorter på helhet og gode rutiner. Forebyggende sikringstiltak kan av den enkelte oppleves som hindringer i hverdagen - stengsler som er i veien for å få jobben gjort raskt. Sikringstiltak som ikke er hensiktsmessig og praktisk utformet kan resultere i at man etter beste evne søker å omgå bestemmelser og rutiner. Det er derfor av stor betydning at den enkelte sikkerhetsleder er seg dette bevisst når sikringstiltak og prosedyrer etableres. Videre må det legges vekt på å oppnå aksept for tiltakene slik at terskelen høynes for å omgå sikkerhetsrutiner av bekvemmelighetshensyn.

Denne veilederen er gitt i medhold av lov om forebyggende sikkerhetstjeneste § 9 og innholdet er i hovedsak relatert til kapittel 6 i forskrift om informasjonssikkerhet. Krav, anbefalinger og veiledning omfatter alle sektorer og virksomheter der skjermingsverdig informasjon behandles. Det presiseres for ordens skyld at veilederen dekker forskriftens krav til sikring av skjermingsverdig informasjon, og ikke virksomhetene selv som fysiske objekter eller deres funksjon.

Dersom det i forbindelse med sikkerhetsrevisjon avdekkes behov for fysiske sikringstiltak utover de som er omhandlet i denne veiledningen, kan NSM bistå virksomhetene med råd. Direktoratets felles e-postadresse er post@nsm.stat.no og på vår hjemmeside www.nsm.stat.no finnes ytterligere informasjon og linker til relevante lover, forskrifter og andre veiledninger og publikasjoner innen NSMs ansvars- og myndighetsområde. For ytterligere praktiske tips om fysiske sikringstiltak anbefaler NSM Forsvarsbyggs sikringshåndbok. Boken er unntatt offentlighet og primært beregnet på Forsvaret, men vil også ha nytteverdi for sivile virksomheter.

2 Generelt om behandling og oppbevaring av sikkerhetsgradert informasjon

Forskriftens grunnregel, inntatt i § 6-1, er at sikkerhetsgradert informasjon og sikkerhetsgodkjente informasjonssystemer kun skal oppbevares eller behandles innenfor område definert som beskyttet eller sperret. Informasjonen kan likevel være i personlig varetekt utenfor disse områdene i forbindelse med reiser, møter, og lignende dersom det er et tjenstlig behov for det. Ved medbringelse av sikkerhetsgradert informasjon gjelder forskriftens kapittel 4, §§4-18 til 4-23. Der gis retningslinjer for hvordan man skal registrere de medbrakte dokumenter ved arkivet samt hvordan man skal forholde seg ved eventuell oppbevaring av dokumenter, bærbare PC'er osv under reisen.

Det er etter at forskriften trådte i kraft akseptert behov for endringer grunnet økende bruk av hjemmekontorer og opprettelse av provisoriske arbeidsplasser i f m prosjekter osv. Det er derfor fremmet forslag om en endring av §§6-1 og 6-10 som vil tillate at sikkerhetsgradert informasjon på mer permanent basis behandles og oppbevares utenfor virksomhetens faste lokaler etter godkjenning gitt av NSM.

En presiserer at omtalte endringer pr. dato ikke er vedtatt i departementet, og at eventuelle ønsker om dispensasjoner fra gjeldende forskrift derfor må behandles av NSM fra sak til sak for å klarlegge individuelle behov og krav til sikring.

3 Inndeling og sikring av fysiske områder

Alle virksomheter som oppbevarer eller tilvirker sikkerhetsgradert informasjon plikter å dele inn sine lokaler i fysiske områder. Områdene skal defineres som henholdsvis kontrollert, beskyttet eller sperret – hvorav kontrollert er det minst vitale og sperret mest sensitivt.

Inndeling i fysisk avgrensede områder er av grunnleggende betydning for å kunne ivareta kravene til sikring på en hensiktsmessig måte. Det er av stor viktighet at denne inndelingen, som blant annet innebærer restriksjoner for den enkeltes adgangsrettigheter, er vel forankret i virksomheten og at den er hensiktsmessig utformet slik at administrasjonen av tilgangsrettigheter blir oversiktlig og enklest mulig.

3.1 Definisjon av de enkelte områder

Sperret område defineres i forskriften som *område hvor adgang gir direkte tilgang til sikkerhetsgradert informasjon*. Typiske sperrede områder er arkiver og dokumenthvelv, operasjonsrom, kommunikasjons- og serverrom eller lokaler der det lages sikkerhetsgraderte produkter. Dette er altså spesialrom hvor sikkerhetsgradert informasjon er åpent eller lett tilgjengelig for den som har adgang.

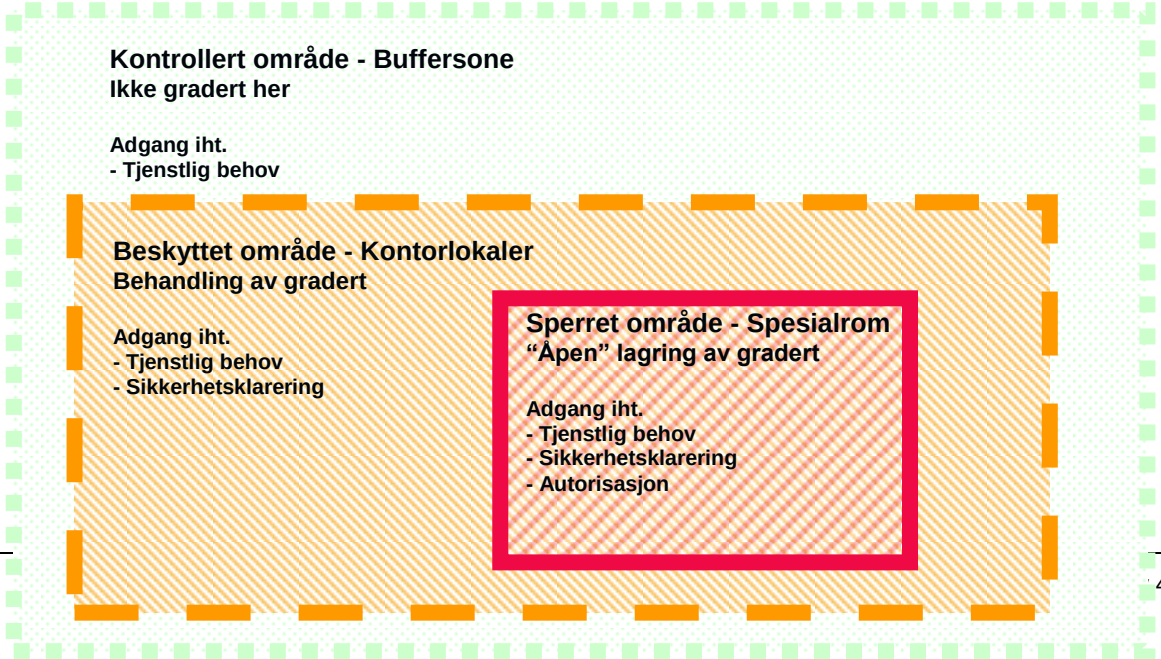
Felles for disse rommene er at det personellet som gis adgang skal være autorisert for den informasjonen og det utstyret som er i rommet.

Beskyttet område defineres i forskriften som *område hvor det behandles eller oppbevares sikkerhetsgradert informasjon eller sikkerhetsgraderte informasjonssystemer*. Den vanligste formen for beskyttet område er kontorlokaler der personellet har gradert PC eller på annen måte behandler gradert informasjon. Den graderte informasjon skal ivaretas av den enkelte, og papirer eller harddisker låses inn i et sikkerhetsskap eller annet når brukeren ikke er tilstede.

De som gis permanent adgang (har egen nøkkel / adgangskort og kan ferdes fritt alene) skal ha gyldig sikkerhetsklarering.

Kontrollert område defineres i forskriften som *område som omgir beskyttet eller sperret område*. Et kontrollert område fungerer som en buffersone mellom område med allmenn ferdsel og de rom hvor det behandles gradert informasjon ved at adgang skal begrenses til de som har et tjenstlig behov for opphold.

Nedenfor er en prinsippskisse som illustrerer soneinndelingen.



Prinsippinndelingen bidrar til redusert trussel ved at personer uten sikkerhetsklarering ikke gis uforstyrret adgang til å tukle med låsene inn til sperrede rom og oppbevaringsenheter.

Inndeling og adgangsbegrensning reduserer også antallet potensielle insidere, eller andre over gjennomsnittet nysgjerrige, som gis anledning til opphold i det beskyttede området og kan plante eksempelvis tasteloggere eller på annen måte å forsøke å tilegne seg informasjon, nøkler og koder. Prinsippet bidrar også til å redusere sannsynligheten for skade dersom gradert informasjon håndteres uforsiktig og tilfeldig kommer uautoriserte i hende.

Ved arealplanlegging og romfordeling bør man prøve å samlokalisere personell slik at praktisk og smidig utførelse av arbeidsoppgaver forenes med personellets sikkerhetsrelaterte autorisasjoner.

- Fellesrom og møterom som er beregnet for ugraderte samtaler og besøkende bør plasseres utenfor beskyttet område. Dette reduserer behovet for ledsaging og kontroll med besøkende og personell uten klarering.

- Kontorer for personell som ikke håndterer sikkerhetsgradert informasjon bør ligge utenfor beskyttet område. Dette fordi det normalt ikke kan kreves at dette personellet skal kunne sikkerhetsklareres.

- Kontorer for personell som skal håndtere gradert informasjon skal plasseres innenfor beskyttet område. Dersom det er noen som ofte håndterer mye og høyt gradert informasjon kan de med fordel ha kontorer i en egen sone. Dette reduserer risikoen for insidehandlinger og tilfeldige kompromitteringer i det beskyttede området for øvrig.

- Møterom beregnet for graderte presentasjoner, videokonferanserom og andre spesialrom med behov for særlig sikring mot avlytting må plasseres innenfor beskyttet område. De bør i tillegg plasseres i et område med liten gjennomgangstrafikk og slik at det ikke er naturlig med opphold tett inntil dører og vegger. Dette for å redusere muligheten for teknisk avlytting og tilfeldig overhøring.

3.2 Kontroll med adgangen til de enkelte områder

3.2.1 Kontrollert område

Den enkelte virksomhet må ta stilling til hvorvidt det er behov for å utøve kontroll i en normalsituasjon, eller om den kan innføre kontroll på et eller annet tidspunkt. En risikovurdering utarbeidet i samsvar med krav i forskrift om sikkerhetsadministrasjon vil gi svar på dette. Det vil i de fleste tilfeller være naturlig at adgangen til området faktisk kontrolleres. Dette kan gjøres ved bruk av vakt eller resepsjon, eventuelt ved hjelp av rotasjonsgrind eller lignende teknisk innretning slik at kun personell med tjenstlig behov får adgang. For å styrke kontrollen utenom arbeidstid kan det også være hensiktsmessig å komplettere med inspeksjoner eller vaktrunder. Et passende deteksjonssystem kan i denne sammenheng vurderes installert. Dersom det kontrollerte området ikke er fysisk avgrenset med etablert adgangskontroll kan dette nedføre større behov for kontroll med beskyttet område. Aktuelle kontrollpunkter kan være dører, vinduer, luker og kabel-/fiberkummer etc.

3.2.2 Beskyttet område

Det skal etableres kontroll med adgangen til beskyttet område. Behovet for kontrolltiltak vil naturligvis variere alt etter virksomhetens størrelse og type, men vil normalt bestå i bruk av vakt, resepsjon, elektronisk adgangskontrollanlegg med kort/PIN eller lignende. Hovedsaken er at tiltakene skal hindre at uvedkommende får adgang uten at det oppdages. Personell som gis permanent adgang skal være sikkerhetsklarert for minimum KONFIDENSIELT. Med permanent adgang menes at man har fått utlevert nøkkel, adgangskort eller lignende og kan komme og gå etter eget ønske. Krav om sikkerhetsklarering gjelder alt personell, også vakter, vedlikeholds- og rengjøringspersonell. Dersom

virksomheten ikke har informasjon gradert høyere enn BEGRENSET gjelder ikke kravet om sikkerhetsklarering for å få permanent adgang.

Det stilles krav til at alle besøkende til beskyttet område skal registreres. Som et minimum bør registreringen omfatte navnet på den besøkende, firma/organisasjon denne representerer, navnet på den som tar imot besøket samt tidspunkt for inn- og utpassering. Dersom det er uhensiktsmessig å benytte en tradisjonell besøksprotokoll, regnes en elektronisk registrering i forbindelse med utlevering av et besøkskort som tilstrekkelig. Kortet kan gjerne utleveres allerede ved innpassering i kontrollert området, avhengig av hva som er mest hensiktsmessig ved den enkelte virksomhet.

Med besøkende menes alle som ikke er gitt permanent adgang. Det kreves at besøkende skal ledsages av personell med permanent adgang. Dette betyr i praksis at den besøkende må møtes ved inngangen og tas hånd om under hele oppholdet. Virksomhetens leder kan likevel for det enkelte tilfelle godkjenne besøk uten ledsagelse, dersom den besøkende er sikkerhetsklarert.

Det stilles krav om at adgangskort og besøkskort skal benyttes og bæres synlig i beskyttet område. Dette kravet kan fravikes dersom den aktuelle virksomheten er så liten at alle med permanent adgang kjenner hverandre av utseende. Det anbefales at besøkskortene utformes slik at det er klart synlig om den besøkende skal ledsages, eller om vedkommende er gitt tillatelse til å bevege seg fritt i området uten ledsagelse. Bruk av forskjellig farge på kortene samt med tekst eksempelvis ”Besøkende med følge” er en vanlig løsning.

3.2.3 Sperret område

I motsetning til beskyttet område, vil sikkerhetsgradert informasjon i et sperret område normalt ikke være nedlåst eller tildekket. Ved å tre inn i området vil man da få tilgang til gradert materiale. Personell som gis adgang skal derfor være autorisert for den informasjonen som befinner seg i området. Det skal foreligge en liste over personell som har permanent adgang, og beslutning om å gi permanent adgang skal tas av virksomhetens leder. Som for beskyttet område kan besøkende gis adgang dersom de legitimerer seg, registreres i protokoll eller lignende og ledsages av personell med permanent adgang. Det er ikke adgang til besøk i sperret område uten ledsagelse. For sperret område kommer i tillegg at sikkerhetsgradert informasjon må låses ned, tildekkes, eller på annen måte gjøres utilgjengelig for den besøkende. NSM legger til grunn at besøk i sperret område utelukkende kan gjennomføres når det foreligger et tjenstlig behov for dette.

Tilgang til sikkerhetsgradert informasjon skal utelukkende gies ut ifra et tjenstlig behov for selve informasjonen. Vakter, vedlikeholdspersonell eller rengjøringspersonell kan derfor ikke gis permanent adgang til sperret område, men må utføre sine oppgaver under oppsyn av autorisert personell.

For å lette den daglige kontrollen bør en datert og signert adgangsliste være oppslått på innsiden av døren inn til området. I tillegg anbefales det at døren merkes med eksempelvis ”Sperret område – adgang kun for autorisert personell” eller annen nøytral formulering som ikke direkte angir rommets innhold.

3.3 Sikring av de enkelte områder

3.3.1 Kontrollert område

Fysisk sikring av et kontrollert uteområde kan for eksempel foretas ved oppsetting av gjerde. Hvilken type av gjerde som skal benyttes må vurderes i hvert tilfelle. Type gjerde avhenger av hvilken funksjon det skal ha og avhengig av trussel er det flere gjerdetyper å velge mellom.

I noen tilfeller kan det være tilstrekkelig med et lavt og enkelt gjerde som avgrenser alminnelig ferdsel. En tydelig fysisk avgrensning med tilhørende merking vil forenkle kontroll og tjene en juridisk hensikt i det området virksomheten har en eierrådighet over identifiseres. I kraft av eierrådigheten kan personer nektes adgang og bortvises. Inntrengen i et fysisk avgrenset område vil etter omstendighetene også kunne være straffbart.

Dersom hensikten er å forsinke eller hindre uvedkommende i å ta seg inn på det kontrollerte området kan høyere flettverksgjerder med klatrehinder benyttes. I denne kategorien finnes også mer solide gjerder som er motstandsdyktige mot klipping og skjæring. Disse benyttes i hovedsak sammen med et deteksjonssystem.

Dersom trusselen skulle tilsi det kan det monteres høysikkerhetsgjerder som er konstruert for å hindre gjennomtrengning med kjøretøyer.

En risikovurdering utarbeidet i samsvar med krav i forskrift om sikkerhetsadministrasjon vil gi svar på hvilken type gjerde som bør benyttes. Eventuelt om det anses tilstrekkelig med vakthold og oppsyn.

3.3.2 Beskyttet område

Forskriften krever at *beskyttet område skal ha en fysisk avgrensning*. Det fysiske skillet mot andre områder vil normalt bestå av gulv, tak, vegger, vinduer og dør. Da det ikke skal være mulig å ta seg inn uten at det kan oppdages skal denne avgrensningen være hel. Dette innebærer blant annet at vegger skal gå over nedsenket himling og under hevet gulv (datagulv). Der dette ikke er praktisk gjennomførbart kan vegg over himling og under gulv erstattes med gitter eller lignende. Konstruksjonen skal være slik at bygningselementer ikke enkelt kan fjernes for så å bli satt tilbake på plass uten at det settes visuelle spor. Dette kan gjøres ved at rommets vegger / plater der det er mulig monteres fra innsiden. For vinduer kan det være hensiktsmessig å benytte enveisskruer i listverket, og dersom de kan åpnes bør det monteres innvendig vinduslås.

I tillegg til den fysiske konstruksjonen bør enkeltkontorer innredes slik at det sikres mot innsyn, også internt, for å oppnå en god beskyttelse mot tilgang til sikkerhetsgradert informasjon fra uautoriserte og besøkende.

3.3.3 Sperret område

Adgang til et sperret område gir direkte tilgang til det sikkerhetsgraderte materialet som befinner seg der. Krav til den fysiske sikringen vil derfor være de som er gjeldende for den høyeste tilgjengelige sikkerhetsgraderingen i rommet.

3.3.3.1 Sperret område for BEGRENSET

For sikring av sperret område / rom for informasjon med laveste gradering benytter forskriften begrepet ”avlåst”. Det stilles ikke spesielle minimumskrav til rommets motstandsevne mot innbrudd og krav til sporbarhet utover de som gjelder for beskyttet område.

Se også veilederens kapittel om låser.

3.3.3.2 Sperret område for KONFIDENSIELT

Et sperret område for oppbevaring av KONFIDENSIELT skal være forsterket mot innbrudd. Forsterkning av vegger skal omfatte hele området fra fast gulv til fast tak, altså gå over senkede himlinger og under hevede gulv (datagulv). Det vil gi en sikkerhetsmessig gevinst om veggene konstrueres av ulike materialer slik at en inntrenger må benytte ulike verktøytyper for å trenge gjennom. I tillegg til forsterkning skal rommet konstrueres slik at uvedkommende ikke får adgang uten at det etterlater tydelige visuelle spor. Oppføringen av rommet må da gjøres på en slik måte at ikke veggplater, vinduer, gitre etc. kan demonteres fra utsiden ved å fjerne lister og skruer for deretter å sette disse på plass igjen. Eksempler på tilfredsstillende veggkonstruksjoner er:

Reisverk av stålstendere med avstand 300mm kledd med 12mm tykke kryssfinerplater på hver side. Finerplatene kan byttes ut med 3mm stålplater med gipskledning. Utvendige skruer bør være av typen enveis. Alternativt kan skruenes skrutrekkerspor freses ut etter montering.

Massive vegger av lecablokker eller murstein kan også benyttes. Disse bør har armering i minimum hvert tredje skift.

Dersom en eksisterende vegg skal forsterkes kan dette gjøres ved montering av 3mm stålplate og ny kledning på rommets innside. Et annet alternativ kan være å sette opp en finerkledd tilleggsvegg med forskjøvet stenderverk mot den eksisterende veggen.

Vindusglass skal tilfredsstille kravene til innbruddsikring minimum klasse B1 etter norsk standard NS-3217 eller klasse P6B etter europanorm EN-NS 356. Det er viktig å påse at innfesting av glass, ramme og karm utføres slik at det ikke svekker motstandsdyktigheten mot innbrudd. Innsetting av sikkerhetsglass bør derfor normalt innebære skifte av ramme / karm samtidig. Vinduer med åpningsmulighet skal påsettes innvendig vinduslås dersom de enkelt kan nås fra bakken eller utspring etc.
Dersom man ønsker å beholde allerede installerte vinduer av svakere kvalitet i et rom som skal sikres, kan det alternativt ettermonteres FG-godkjent gitter/ sjalusi.

Dører skal være forsterket utover normal bygningsstandard og fortrinnsvis bør en sikkerhetsdør benyttes. En sikkerhetsdør klasse 2 etter standard NS-3170 er et eksempel på tilfredsstillende dør. Se også eget kapittel om dører.

For avlåsning kreves låsetøy godkjent av NSM. For graderingsnivået KONFIDENSIELT vil dette normalt si FG-godkjente sikkerhetslåser. Det presiseres at det ikke tillates at låsetøyet er på system - det er kun tillatt med "unike" låser for hvert enkelt sperret område. Likelåsende sylindere kan likevel benyttes der hvor dette ikke kommer i konflikt med prinsipper om autorisasjon i henhold til tjenstlig behov.
Ved bruk av godkjent tastaturlås må denne være plassert på en slik måte at uautorisert visuell avlesning ved tasting av koden vanskeliggjøres. Bruk av låsens medfølgende tastaturavskjerming bør benyttes. Videre bør tilgangen til området rundt være begrenset for å minimere muligheten for preparering og teknisk avlesning av tastaturet. Se forøvrig veilederens kapittel om låsetøy.

Forskriften tillater konstruksjon med lavere styrkegrad dersom det av bygningstekniske årsaker er nødvendig og dersom tilsyn og reaksjonsapparat gjør dette forsvarlig. I de fleste tilfeller vil dette si tilstedeværelse av vaktpersonell i umiddelbar nærhet. Se også veilederens avsnitt om tilsyn.

3.3.3.3 Sperret område for HEMMELIG

Et sperret område for HEMMELIG skal sikres som hvelv. NSM er godkjenningsmyndighet for spesifikasjoner for hvelv, jf § 6-14.

Som hvelv godkjenner NSM prefabrikkerte hvelv med styrkegrad som tilfredsstiller kravene til klasse 2 eller høyere etter standard NS-EN 1143-1.

I mange tilfeller vil plasstøpte hvelv eller egenkonstruerte strongrooms være et alternativ til prefabrikkerte elementhvelv. Krav til styrke kan variere avhengig av plassering og omgivelser, men som en rettesnor kreves normalt vegger i minimum 100 mm betong B30 med armering 8x150x150. Gulv og tak skal konstrueres slik at de ikke utgjør en svekkelse ift dette kravet. Alternativt til armert betong kan det benyttes sammensatte vegger. En konstruksjon bestående av 2mm stålplate, en kjerne av spon, kryssfiner og/eller polykarbonat, samt 4mm plate i herdet stål og gipskledning på begge sider vil gi tilfredsstillende innbruddstyrke.

Forskriften tillater konstruksjon med lavere styrkegrad enn ovennevnte dersom det av bygningstekniske årsaker er nødvendig, og dersom tilsyn og reaksjonsapparat gjør dette forsvarlig. Det er da et krav at reaksjonstiden skal være kortere enn innbruddstiden. I de fleste tilfeller vil dette si tilstedeværelse av vaktpersonell i umiddelbar nærhet. Se også veiledningens avsnitt om tilsyn. Det presiseres at døren uansett skal utstyres med 2 godkjente låser. For valg av dør og låsetøy; Se egne kapitler i denne veilederen.

3.3.3.4 Sperret område for STRENGT HEMMELIG

Kravet til et sperret område for oppbevaring av den høyeste graderingen er skjerpet i f t kravene for HEMMELIG. Det kreves da at rommet som minimum er oppført i h t godkjent spesifikasjon for hvelv, lettere konstruksjoner tillates ikke.

I tillegg til dette skal det etableres permanent vakthold eller installeres elektronisk sikringsanlegg.

Et elektronisk sikringsanlegg skal som minimum dekke arealet rundt hvelvet og hvelvdøren og termineres i bemannet vakt der det skal foreligge plan for reaksjon. Beregnet maksimum reaksjonstid skal være kortere enn beregnet innbruddstid.

Hensikten med sikringen er å hindre tilgang til den graderte informasjonen. Det er derfor ikke tilstrekkelig med eksempelvis bevegelsesdetektorer på innsiden av hvelvet eller magnetkontakt på hvelvdøren for å registrere at innbrudd har funnet sted, men anlegget skal også kunne detektere og varsle om forsøk på innbrudd eller uønsket tilstedeværelse i hvelvets umiddelbare nærhet. Se veiledningens kapittel om elektroniske sikringsmidler.

Kravet til vakthold og plan for reaksjon må forstås slik at det skal foreligge reell evne til å forhindre at innbruddsforsøket lykkes.

3.3.4 Tilsyn

Forskriftens § 6-8 sier blant annet følgende om sikring av beskyttet område: *"Dersom det er KONFIDENSIELT eller høyere i området skal det føres tilsyn med området."* Hensikten med bestemmelsen er å sikre et minimumsnivå av tilsyn ved virksomheter som oppbevarer informasjon gradert f.o.m. KONFIDENSIELT i sine lokaler. Kravet gjelder også for sperrede områder, men da disse normalt befinner seg inne i beskyttet område er tilsvarende formulering ikke tatt inn i § 6-9.

Forskriftens § 6-9 om sperret område omtaler også krav til tilsyn i 7. ledd. "*Det skal etableres permanent vakthold eller installeres et elektronisk sikringsanlegg. Et elektronisk sikringsanlegg skal som minimum dekke arealet rundt hvelvet og hvelvdøren og termineres i bemannet vakt der det skal foreligge plan for reaksjon. Beregnet maksimum reaksjonstid skal være kortere enn beregnet innbruddstid."* Dette kravet gjelder i utgangspunktet for informasjon gradert STRENGT HEMMELIG og hensikten er å sikre umiddelbar og tilstrekkelig reaksjon. Dette kravet om tilsyn/reaksjon er altså ikke det samme som det grunnleggende tilsynet i § 6-8.

3.3.4.1 Former for tilsyn

Formålet med tilsynet er at sikkerhetstruende hendelser og innbrudd skal kunne oppdages innen rimelig tid. Med dette må forstås at området holdes under oppsyn etter normal arbeidstid, i helger, og i ferieperioder etc. Mulige tilsynsformer kan være stedlig vakt, vaktrunder / patruljering, innbruddsalarmanlegg, eller kameraovervåking. Det bør dokumenteres ved rundeprotokoll eller annen registreringsmetode at kontrollene faktisk har funnet sted. Detaljkontroll av låsingen av skuffer og skap bør vurderes gjennomført i sammenheng med vaktrunde etter normal arbeidstid (OBS vaktens sikkerhetsklarering). Typisk svakere punkter som bør vektlegges er bakdører, rømningsveier, tekniske åpninger (luker, o l som er store nok for en forsering) og vinduer.

Forskrift om informasjonssikkerhet gir ingen konkrete føringer om hva slags tilsyn som til enhver tid er tilstrekkelig. Dette må fremkomme av en risikovurdering for den enkelte virksomhet. Det vises for ordens skyld til forskrift om sikkerhetsadministrasjon kapittel 4 om krav til risikohåndtering og sikkerhetsrevisjon.

4 Oppbevaringsenheter for sikkerhetsgradert informasjon

4.1 Oppbevaringsenheter for BEGRENSET

Minimumskravet til oppbevaring er satt ved å benytte begrepet "avlåst". Utover dette stiller ikke forskriften spesielle krav hverken til låsens kvalitet eller skapets eller rommets fysiske motstandsevne mot innbrudd. Enkle oppbevaringsenheter og eksempelvis en skuff i et kontormøbel kan imidlertid være konstruert slik at det er mulig å fiske ut dokumenter via sprekker eller ved å fjerne andre skuffer, bakplater etc. Denne type møbler bør unngås brukt til oppbevaring av sikkerhetsgradert informasjon.

4.2 Oppbevaringsenheter for KONFIDENSIELT

Oppbevaringsenheter for informasjon gradert KONFIDENSIELT skal være godkjent av NSM, jf § 6-14.

Oppbevaringsenhetene kan deles i to hovedgrupper: tynnplateskap og sikkerhetsskap (eller verdiskap).

For oppbevaring av KONFIDENSIELT tillater NSM bruk av alle verdiskap som innehar en klassifisering etter standard NS-EN 1143-1, samt alle FG-godkjente sikkerhetsskap.

Tynnplateskap som er godkjent av NSM er:

- Modellserie FOSSAFE K-skap fra firma Finn Clausen Arkivsystemer AS. Disse kommer både som skuffeseksjoner, hurts og høyskap med hyller. Skapene leveres med nøkkellås merke KABA Titan, eller elektronisk kombinasjonslås merke Wittkopp Combistar.

- Skuffeseksjon RSH 2000 NF fra firma Robur Safe AS. Disse kommer i 2 og 4 skuffers versjon og leveres med elektronisk kombinasjonslås som trenger ekstern strømforsyning (220V AC).

Dersom det ønskes benyttet andre skap til oppbevaring av KONFIDENSIELT skal disse fremmes NSM for godkjenning. Ved søknad om godkjenning vil følgende forhold ved konstruksjonen tillegges særlig vekt:

- Oppbevaringsenheten må produseres i stålplater hvis minimum tykkelse ikke er under 1mm.

- Karmer, dører og skuffefronter må være falset eller avstivet/forsterket slik at oppbrekking vanskeliggjøres.

- Det må ikke være mulig å hente/”fiske” sikkerhetsgraderte dokumenter via sprekker rundt skapdører, skuffer eller andre åpninger.

- Alle sammenføyninger må sveises / tilsvarende på en slik måte at demontering utenfra utelukkes uten samtidig å ødelegge skapet.

- Dørhengsler må skjules / dekkes eller utformes slik at åpning ved fjerning av hengsel utelukkes.

- Mekanisme for avlåsning bør være flerpunkts og med avlastet / indirekte kobling til låsen.

- Oppbevaringsenheten må utstyres med godkjent lås. (Se veilederens kapittel om låser).

Tidligere gitte enkeltgodkjenninger (skriftlige) av tynnplateskap er fortsatt gjeldende ved den virksomhet der godkjenningen ble gitt.

NSM anbefaler at tynnplateskap kun benyttes der hvor sikringen av det beskyttede området anses for å være god, eller hvor det vurderes å være en lav risiko ved innbrudd. I motsatt fall bør det benyttes verdi- eller sikkerhetsskap.

Låser til oppbevaringsenheter skal ikke være i et låssystem - det skal være ”unike” låser for hver enkelt oppbevaringsenhet. Likelåsende sylindere kan likevel benyttes der hvor dette ikke kommer i konflikt med prinsipper om autorisasjon i henhold til tjenstlig behov. Ved bruk av skap med kombinasjonslås bør dette plasseres på en slik måte at uautorisert visuell avlesning av koden vanskeliggjøres. Bruk av tastaturskjerm eller lignende bør benyttes. Videre bør tilgangen til rommet være begrenset for å redusere muligheten for preparering og teknisk avlesning av tastaturet. Se for øvrig denne veiledningens kapittel om låser.

4.3 Oppbevaringsenheter for HEMMELIG

Oppbevaringsenheter for informasjon gradert HEMMELIG skal være godkjent av NSM, jf § 6-14.

For oppbevaring av HEMMELIG tillater NSM bruk av alle verdiskap som innehar en klassifisering minimum klasse 1 etter standard NS-EN 1143-1. Dersom skapet veier mindre enn 300 kg skal det boltes fast. Tilsvarende som for hvelvdører skal skapet utstyres med to godkjente låser. Se denne veiledningens kapittel om låser godkjent for HEMMELIG.

I tillegg har NSM godkjent en serie eldre(nå utgåtte) spesialkonstruerte skap fra firma JØLI Safe - modellene M5 A, B og C.

Dersom det er behov for å benytte andre typer enheter for oppbevaring av HEMMELIG skal disse fremmes NSM for godkjenning. Ved søknad om godkjenning vil følgende forhold ved konstruksjonen tillegges særlig vekt:

- Oppbevaringsenheten bør ha innbruddsstyrke tilsvarende som verdiskap etter NS-EN 1143-1 minimum klasse 1.
- Alle sammenføyninger må konstrueres på en slik måte at demontering utenfra utelukkes uten samtidig å ødelegge skapet.
- Det må ikke være mulig å tilegne seg gradert informasjon ved å innføre prober eller annet teknisk utstyr gjennom sprekker, ventilasjonskanaler, kabelgjennomføringer eller andre åpninger.
- Det må ikke være mulig å manipulere sikkerhetsgradert utstyr (eksempelvis server, nettverkskomponenter med mer) ved å innføre prober eller annet teknisk utstyr gjennom sprekker, ventilasjonskanaler, kabelgjennomføringer eller andre åpninger.
- Oppbevaringsenheten må utstyres med godkjente låser. (Se veilederens kapittel om låser).
- Oppbevaringsenheten bør utstyres med innslags- og borsikringer for låser og låsemekanisme.

Tidligere gitte enkeltgodkjenninger (skriftlige) av oppbevaringsenheter for HEMMELIG er fortsatt gjeldende ved den virksomhet der godkjenningen ble gitt.

Safe for nettverksutstyr/servere gradert HEMMELIG. NSM har godkjent følgende safer konstruert for formålet:

- PSSO AS – «Serversafe 19»
- Robur Safe AS- «RVH-SH-800»

4.4 Oppbevaringsenheter for STRENGT HEMMELIG

For oppbevaring av STRENGT HEMMELIG godkjennes bruk av samme type oppbevaringsenheter som for HEMMELIG. Skapet skal plasseres i et sperret område sikret for minimum KONFIDENSIELT.

Tilsvarende som for hvelv for STRENGT HEMMELIG skal det også her etableres permanent vakthold eller installeres elektronisk sikringsanlegg med samme krav til varsling og reaksjon.

5 Sikring av informasjonssystemer, kabelsystemer og nettverkskomponenter

Krav til sikring av kabler og nettverkskomponenter i et informasjonssystem er regulert i flere deler av forskrift om informasjonssikkerhet samt i Vedlegg 1, som blant annet inneholder disse overordnede bestemmelsene:

§2-1. "Kabelsystem og andre installasjoner skal installeres slik at de hindrer uvedkommende å få tilgang til systemet, sende uautorisert informasjon gjennom systemet, eller å skade systemet. Sikringen kan bestå av en kombinasjon av forseringshindringer, tilsyn og fysisk kontroll".

§2-3. "Kabelsystemet skal i sin helhet legges innenfor kontrollert område. I kabelsystemet skal omformere, tilkoblingsutstyr og tilkoblingspunkter plasseres innenfor beskyttet eller sperret område, og uvedkommende hindres adgang ved avlåsing. NSM kan bestemme hvilke typer forseringshindre, herunder kummer og skap, som kan benyttes til sikring av kabelsystem".

Behovet for sikring av de enkelte deler av et informasjonssystem vil avhenge av graderingsnivå, komponenttype, konfigurasjon og type trafikk på den enkelte kabel.

5.1 Kabler

Sikkerhetsgraderte kabelsystemer skal i sin helhet legges innenfor minimum kontrollert område. Kabler som plasseres utendørs, skal ligge nedgravd på oversiktlige steder der det er lett å kontrollere om graving har funnet sted. Innendørs skal kabler legges i separate rør eller kanaler som enkelt muliggjør kontroll. Bestemmelsen gjelder alle typer gradert kabel, også optisk fiber. Hensikten med å benytte egne rør og kanaler er i første rekke å oppnå bedre oversikt og separasjon fra ugradert kabling, men kanaler kan godt legges i samme kabeltrase som annen kabel. Det kan være at deler av kabelsystemet er forbundet med større risiko, eksempelvis tapping av fiber som overfører sentral backup eller lignende. Særlig risikoutsatte kabler kan behøve ytterligere sikring mot fysisk tilgang. Se eget avsnitt om risikohåndtering i dette kapittelet.

I rom i utlandet skal kabelsystemer for graderte informasjonssystemer ikke installeres som skjult anlegg. Det samme gjelder for installasjoner i permanent sikrede konferanserom og spesialrom som faller inn under forskriften kapittel 9.

Det skal foreligge et kart over kabelsystemet. Kabelkartet skal gi opplysninger om trasèer, plassering av omformere, tilkoblingsutstyr, tilkoblingspunkter, kummer og skap, og overganger mellom ute- og inneområder. Kabelkartet skal sikkerhetsgraderes minimum BEGRENSET.

5.2 Kummer

Avlåsing kan f eks skje med en tverrstang over kumlokket. Helst bør det benyttes et eget underlokk laget at hardt stål, minimum 5mm tykt. Av praktiske årsaker vil det som oftest være vanskelig å benytte andre låstyper enn hengelåser. Disse må være av FG-godkjent type og beregnet for utendørsbruk. NSM anser at låsens kvalitet bør være minimum FG-klasse 3 til dette formålet. Låsen bør i tillegg beskyttes/dekkes med et beslag som er like sterkt som selve lokket den skal sikre. Beslaget bør dekke så mye av låsen og låsemekanismen som mulig.

Siden en kum i de fleste tilfeller vil være sårbar pga utsatt plassering må den overvåkes, f.eks. med hyppig kontroll av vakt eller ved bruk av alarmanlegg. Se også veilederens avsnitt om tilsyn og elektroniske sikringsmidler.

5.3 Nettverkskomponenter

Alle nettverkskomponenter skal som et minimum plasseres under egen avlåsing, i eget rom eller skap, innenfor beskyttet eller sperret område.

Kravet til plassering og egen avlåsing av nettverkskomponenter er minimumstiltak basert på en generell risikovurdering.

Ekstra sikringstiltak kan være en kombinasjon av fysiske og logiske sperrer samt kontrolltiltak. Dersom det er behov for øket fysisk kontroll med nettverkskomponentene kan rom eller oppbevaringsenheter forsynes med alarm eller annen overvåking. Som eget tiltak eller i kombinasjon med øket kontroll kan det være behov for å benytte forsterkede rom eller oppbevaringsenheter. Dette må naturligvis velges etter bl.a. volumbehov og muligheter for modifisering siden det er behov for gjennomføring av kabler. For eksempel kan tradisjonelle verdiskap for oppbevaring av HEMMELIG informasjon være uhensiktsmessige til dette spesielle behovet, bl.a. fordi de er konstruerte for å motstå boring. Skaptypen som i mange tilfeller kan være aktuell er derfor et FG-godkjent sikkerhetsskap/serverskap med tilleggsmontert kombinasjonslås godkjent av NSM. Disse skapene er normalt bygget opp av stålplater uten betongfylling, og lar seg lett modifisere med tanke på kabelgjennomføringer. Enkelte modeller er konstruert for oppbevaring av operativt datautstyr og er derfor utstyrt med ventilasjon eller kjøling. Oppbevaringsenhetene må plasseres i minimum BESKYTTET område. Dersom rom skal forsterkes eller andre typer skap av praktiske grunner ønskes benyttet, bør NSM konsulteres på forhånd.

5.4 Servere

Servere skal installeres i et serverrom som er sikret iht. kravene for den høyeste sikkerhetsgradering som systemet skal godkjennes for. Se veilederens kapitler om sikring av sperret område. Dersom et eget serverrom ikke kan benyttes, kan en godkjent oppbevaringsenhet plassert i minimum BESKYTTET område brukes.

5.5 Brukerterminaler/kontorer

Brukerterminaler kan være utsatt for manipulering. Det er eksempelvis en smal sak for en eventuell insider å montere tasteloggere eller annet utstyr. Som et risikoreduserende tiltak er det derfor en fordel at kontorer holdes låst når brukeren ikke er tilstede. Avlåsing av kontordører innenfor beskyttet område er ikke et pålagt minimumskrav, men generelt ønskelig praksis. Nøkkelen må være under kontroll.

5.6 Skrivere

Som andre komponenter kan skrivere tappes for lagret informasjon eller manipuleres. Utskrifter kan også i perioder ligge tilgjengelig for personell uten tjenstlig behov for disse. Printere bør derfor ikke stå i korridorer og lignende, men plasseres på et eget rom. Rommet bør låses av med kodelås eller kobles til adgangskontrollsystemet. I tillegg bør «follow me» print vurderes.

5.7 Risikovurdering og dokumentasjon

Risikohåndtering skal utøves i samsvar med forskrift om sikkerhetsadministrasjon kapittel 4.

Behov for sikring utover det pålagte minimum kan eksempelvis komme av særlig sårbarhet eller konsekvens ved manipulering, eller at det på permanent basis lagres gradert informasjon i komponenten. Risikoen forbundet med den enkelte system- og nettverkskomponent vil variere alt etter komponenttype og hvilket miljø den står i. Det må derfor foretas en vurdering i det enkelte tilfellet. Vurderingen skal foretas av informasjonssystemets eier eller den som er ansvarlig for utviklingen. Hvem dette er må fastslås i godkjenningsstrategien for det enkelte system. Behovet for sikringstiltak for de enkelte komponentene skal fremgå av sikkerhetsdokumentasjonen og kan etterprøves av den som er godkjenningsansvarlig for informasjonssystemet.

NSM er gitt myndighet til å kunne dispensere fra gjeldende krav. En dispensasjon vil kunne vurderes gitt dersom alternative sikkerhetstiltak er begrunnet i en gjennomført risikoanalyse, jf. forskrift om sikkerhetsadministrasjon kapittel 4 om risikohåndtering og sikkerhetsrevisjon.

6 Håndtering av nøkler og koder

Forskrift om informasjonssikkerhet stiller i kapittel 6E krav til håndteringen av nøkler og koder. Bestemmelsene er relativt konkrete og det anses ikke å være behov for å gjengi eller utdype disse i denne veiledningen. Imidlertid vil en presisere at god kontroll og korrekt håndtering er av vesentlig betydning for sikkerheten.

En må være på vakt mot uhjemlet kopiering av nøkler eller nøkkelprofiler da de tekniske hjelpemidlene som behøves er praktisk tilgjengelig for enhver som måtte ønske det. En kopi kan lages ut fra en originalnøkkel som på en eller annen måte avleses. Dette kan gjøres ved avtrykk, avfotografering eller endog ved visuell undersøkelse av en trenet person. Mange typer adgangskort og lignende kan også kopieres. Det er derfor avgjørende at innehaverne er seg dette bevisst når nøkler og kort oppbevares i personlig varetekt.

Nye nøkler kan også lages ut ifra produksjonskoder beskrevet i en nøkkelplan eller lignende hos leverandøren. Eieren av låser og låsesystemer bør derfor treffe tiltak for å sikre mot uønsket kopiering. Bruk av seriøse leverandører, sikker oppbevaring av relevant informasjon om låsesystem, intern instruks for nøkkelhåndtering er da sentrale virkemidler. I denne forbindelsen vil en også minne om at kontrolltiltak ikke bare er til mot eksterne trusler, men også mot potensielle insidere.

I forskriften § 6-17 stilles det krav til kontroll med, og regelmessig opptelling av, nøkler i samsvar med låsplanen. Med nøkler må forstås alle typer, også adgangskort og tilsvarende. Med regelmessig opptelling må forstås minimum årlig, gjerne i forbindelse med årlig sikkerhetsrevisjon.

6.1 Nøkkelskap

Nøkkelskap skal være godkjent av NSM, jf § 6-14. Følgende skap er gitt generell godkjenning.

- Modell T2 deponeringssafe fra firma Myhre Lås & Mek.
- Deponeringssafe gulv- og veggmodell fra firma Jøli Safe.
- Nøkkelskap N-51 fra firma Jøli Safe.

  Disse skapene leveres med sertifiserte (UL,VdS) Sargent & Greenleaf kombinasjonslåser.
- FOSSAFE nøkkelskap modell E K 100 fra firma Finn Clausen Arkivsystemer.

  Skapet leveres med kombinasjonslås Cawi ElCom 7205.
- Robur nøkkelskap RSKN fra firma Robur Safe.

  Skapet leveres med kombinasjonslås Wittkopp Combistar Easy / Primor 2000. Sertifiserte (UL, VdS) Sargent&Greenleaf kombinasjonslåser kan også benyttes.

For oppbevaring av nøkler tillater NSM også bruk av andre oppbevaringsenheter (safer og sikkerhetsskap) så sant disse er FG-godkjent med kombinasjonslås.

Dersom det ønskes benyttet andre nøkkelskap skal søknad om bruk fremmes NSM. Ved søknad om godkjenning vil følgende forhold ved konstruksjonen tillegges særlig vekt:

- Skapet må produseres i stålplater hvis minimum tykkelse ikke er under 1mm.
- Karmer og dører må være falset eller avstivet/forsterket slik at oppbrekking vanskeliggjøres.

- Det må ikke være mulig å hente eller enkelt avfotografere nøkler via sprekker rundt skapdør eller andre åpninger.

- Alle sammenføyninger må sveises / tilsvarende på en slik måte at demontering utenfra utelukkes uten samtidig å ødelegge skapet.

- Dørhengsler må skjules / dekkes eller utformes slik at åpning ved fjerning av hengselstapp utelukkes.

- Skapet må ha kombinasjonslås.

- Mekanisme for avlåsning bør være flerpunkts og med avlastet / indirekte eller kobling til låsreile/tilsvarende.

- Om mulig bør skapet være utstyrt med innretning for individuell avblending av den enkelte nøkkel. Dette for å hindre uautorisert avlesing av nøkkelprofiler/kort.

Enkeltgodkjenninger for bruk av tynnplate-nøkkelskap gjelder ved den virksomhet der godkjenningen ble gitt. Tynnplate nøkkelskap (for eksempel Key Watcher fra firma Mil Sec) bør bare benyttes der hvor sikringen av skapet anses for å være god, (eksempelvis i sikret rom eller bemannet vakt). I motsatt fall bør det benyttes/plasseres i et skap av FG-godkjent / tilsvarende standard

Nøkkelskap bør plasseres slik at uautorisert visuell avlesning av koden vanskeliggjøres. Bruk av tastaturskjerm eller lignende bør benyttes. Videre bør tilgangen til rommet være begrenset for å minimere muligheten for preparering og teknisk avlesning av tastatur.

7 Låser

En leverandør av låsesystemer vil ha alle data om dine låser og dine nøkler i sitt arkiv. Bruk derfor alltid en anerkjent og seriøs leverandør. Det kan av og til være behov for ettermontering av låser på skap og dører som ikke er konstruert for den aktuelle låsen på forhånd. I slike tilfeller er det avgjørende at arbeidet utføres av en kvalifisert håndverker. NSM anbefaler at et kriterium for valg av firma bør være at det er en mesterbedrift med sertifikat fra Norsk låsesmedforening. Dette gir trygghet for godt håndverk og etisk håndtering av informasjon om dine låser.

I det følgende beskrives noen prinsipielle forhold rundt låsetøy samt hva som er godkjent for de enkelte graderinger.

7.1 Avlåsing generelt

En stor andel av begåtte innbrudd skjer ved at låsen ødelegges med fysisk makt, og redskaper som brekkjern, boremaskin og slagverktøy er vanlige hjelpemidler. For at låsen ikke skal fremstå som et svakt punkt for angrep er det derfor viktig at den er minst like motstandsdyktig som døren for øvrig. I tillegg til at låsen skal være solid for å motstå fysisk makt bør den også være vanskelig å manipulere.

Det er store variasjoner i kvalitet på de ulike låsproduktene på markedet, og det kan være vanskelig for ufaglærte å vurdere egenskapene. Låser som er godkjent av forsikringsselskapene har vært gjennom en evaluering som garanterer for en viss motstandevne. Det bør derfor alltid benyttes FG-godkjente sikkerhetslåser i ytterdører og dører inn til beskyttet område.

7.2 Låser for BEGRENSET

Det stilles ingen absolutte krav til låser for denne graderingen. Begrepet ”avlåst” er benyttet i forskriften og anses normalt som tilstrekkelig. Det bør uansett vurderes hvorvidt låsen er av noe kvalitet. Et eksempel på låser uten vesentlig sikkerhetsfunksjon er møbellåser der nøkkelkoden er stemplet utenpå selve låsesylinderen. I et kontorbygg vil det i mange tilfeller være slik at flere låser er like og at flere personer dermed har nøkkel til skuffen. En del av låsene i kontormøbler, rimelige skap

og enkle dører til kontorer og korridorer kan også være av svært enkel konstruksjon og har i sikkerhetsmessig sammenheng liten verdi.

7.3 Låser for KONFIDENSIELT

Låser for denne graderingen skal være godkjent av NSM, jf § 6-18.

For sikring av informasjon gradert KONFIDENSIELT tillater NSM bruk av alle FG-godkjente nøkkellåser / sikkerhetslåser minimum klasse 3 (NS-3620 eller tilsvarende). Det er verdt å merke seg at en lås kan bestå av flere deler som alle skal være godkjent. De aktuelle delene er låskasse, sylinder, beslag og sluttstykke.

Ved bruk av kombinasjonslås skal disse være sertifisert minimum VdS class 2 / EN-1300 class B.

Dersom det er behov for å benytte en lås som ikke innehar FG-godkjenning eller sertifisering som angitt over skal søknad fremmes NSM. Ved søknad om godkjenning må et eksemplar av låsen gjøres tilgjengelig for NSM for tester. Følgende forhold vil tillegges særlig vekt:

- Låsen må være sikret mot angrep med enklere verktøy. Dette innebærer blant annet at sylinderlåser skal være utstyrt med borsikring og sikkerhetsskilt.
- Låsen må ha en viss beskyttelse mot manipulering. Eksempelvis bør sylindere utstyres med spesielle profiler, samt ulike typer stifter og fjærer for å vanskeliggjøre dirking.
- Låsen bør tilfredsstille kravene til FG-klasse 3, (NS-3620 eller tilsvarende).
- Kombinasjonslåser bør ved behov kunne skjermes for avlesning/avtitting av dreieskive, display, tastatur eller tilsvarende.
- Kombinasjoner bør minimum være sekssifret.
- Elektroniske kombinasjonslåser må ha en funksjon som sperrer låsen i x antall minutter etter setting av x antall feilkoder.
- Kombinasjonslåser bør inneha en sikkerhetssertifisering fra et anerkjent sertifiseringsorgan (f.eks. UL, CEN, VdS, etc). Dokumentasjon fra sertifiseringsorganet bør vedlegges søknaden.
- Elektroniske kombinasjonslåser bør vedlegges produsentens tekniske dokumentasjon for elektronisk design/sikkerhetsfunksjoner.
- For biometrisk lås behøves særlig utfyllende dokumentasjon om sikkerhetsfunksjoner mot manipulering.

7.3.1 Valg av låstype

Sylinderlåser er konstruert slik at sylinderen er tilgjengelig fra utsiden av døren. Sylinderkjernen er som oftest produsert i messing og selv om den er forsynt med herdede stålstifter for å vanskeliggjøre utboring vil den utgjøre et svakt punkt for angrep. I tillegg kommer nødvendigheten av nøyaktig tilpassning av sylinder og sikkerhetsskilt (max 2 mm utstikk fra skilt) for å hindre at sylinderen kan slås eller vris i stykker. Der det er hensiktsmessig anbefales derfor at en lås av tilholdertypen benyttes. Disse vil være bedre beskyttet ved at de i sin helhet er montert inne i døren og kun tilgjengelig gjennom nøkkelhullet fra utsiden.

Hengelåser bør kun brukes hvis det er det eneste praktiske alternativet. For tynnplateskap med sperrestag skal den være av type med en viss dirkmotstand. Ett eksempel på slik lås er skivesylinderlås Abloy modell 3020. Andre FG-godkjente hengelåser tillates brukt på tynnplateskap dersom de er utstyrt med sikkerhetssylinder og er uten smekklåsfunksjon. For avlåsing av dør til sperret område skal hengelåsen være FG-godkjent minimum klasse 3 (klasse 4

etter nyere standard NS-EN 12320). Hengelåsbeslaget må i slike tilfeller også være på samme nivå. Hengelåser kan relativt enkelt klippes/kuttes av og erstattes med en tilsvarende lås uten at dette setter spor. Dersom en lås "plutselig" slutter å fungere anbefales det derfor at det tas kontakt med kompetent sikkerhetspersonell eller låsesmed for å vurdere om låsen kan ha vært manipulert eller skiftet ut.

Alle låser til sperrede områder og oppbevaringsenheter for KONFIDENSIELT skal ha unike nøkler - det vil si at de ikke skal være del i et låssystem. Likelåsende sylindere kan likevel benyttes der hvor dette ikke kommer i konflikt med prinsipper om autorisasjon i henhold til tjenstlig behov.

Ved bruk av kombinasjonslåser kan det være risiko for kompromittering av koden ved bruk. Skap / lås bør derfor plasseres slik at visuell avlesning ved tasting av koden anses usannsynlig. Videre bør tilgangen begrenses slik at muligheten for preparering og teknisk avlesning av tastaturet hindres.

7.3.2 Låskasser

Godkjente låskasser leveres i mange utførelser og med flere kombinasjoner av vridere, faller og reiler. Bruksområdene er forskjellige og behovet må vurderes ut ifra hvorvidt døren er beregnet på hyppige opp- og igjenlåsninger, hvorvidt den skal fungere som rømningsvei etc. Eksempelvis vil en låskasse med hakereile normalt gi bedre sikkerhet mot brytning enn en med rett reile. Låser med nøkkelsylinder på begge sider, eventuelt med frakoblingsbar vrider, egner seg best på dører med vindu etc. Selv om de alle er godkjent for bruk, bør en vurdering av låskassens hensiktsmessighet ligge til grunn før valget.

7.4 Låser for HEMMELIG / STRENGT HEMMELIG

For avlåsning av de høyeste graderingene kreves bruk av to låser godkjent av NSM, jf § 6-18. Minst en av låsene skal være en kombinasjonslås.

Det kan av og til være behov for ettermontering av låser på dører som ikke er konstruert for den aktuelle låsen på forhånd. I slike tilfeller er det avgjørende at arbeidet utføres av en kvalifisert håndverker. Forhold som avlastning av låsereiler, tilpassning til reileverk, innslags- og borsikringer bør vektlegges. NSM anbefaler at et kriterium for valg av firma bør være at det er en mesterbedrift med sertifikat fra Norsk låsesmedforening.

7.4.1 Lås # 1, hovedlås

For sikring av graderingene HEMMELIG og STRENGT HEMMELIG har NSM godkjent et begrenset antall kombinasjonslåser:

- Sargent & Greenleaf:
  - Treveis mekaniske dreielåser i modellseriene 8400 MP, 8500 MP og modell 2937.
  Dersom låsen skal monteres på en dør der det er krav til rømning med innvendig vrider, kan tilleggsutstyr Extension 50 brukes.
  - Elektronisk dreielås modell 2740.
  Dersom låsen skal monteres på en dør der det er krav til rømning med innvendig vrider, kan modell Extension 2890 brukes.

-Modell 2740 vanlig og modell 2890 PDL for andre dører

- Kaba Mas:
  - Elektronisk dreielås modell X-09 (samt de utgåtte modellene fra Mas Hammilton) X-07 og X-08).
  Dersom låsen skal monteres på en dør med krav til rømning med innvendig vrider, kan tilleggsutstyr CDX-09 brukes.

- Modell X-10 (for safe og hvelvdør) og CDX-10(samme lås med extention for andre dører)

- NL Lock:
  - Elektronisk lås EM 20
- -20 Rotobolt, i kombinasjon med tastatur Secret BR5020.

- La Gard:
  - Elektronisk lås LGBasic 4200 swingbolt, i kombinasjon med tastatur 3190 PRIVAT II.
  - Elektronisk lås LGBasic 3740 deadbolt, i kombinasjon med tastatur 3190 PRIVAT II
- - 6040M deadbolt med La gard privat II mod 3190 tastatur vribart

- Wittkopp Cawi:
  - Elektronisk lås TwinLock 7220 med panel 7237 Flatcontrol. Disse kan leveres som sett av 2 godkjente låser styrt av samme panel.

Dersom det er behov for å benytte en annen kombinasjonslås skal søknad fremmes NSM. Ved søknad om godkjenning må et eksemplar av låsen gjøres tilgjengelig for NSM for tester. Følgende forhold vil tillegges særlig vekt:

- Kombinasjonslåsen må inneha en sikkerhetssertifisering fra et anerkjent sertifiseringsorgan (f.eks. UL, CEN, VdS, etc). Dokumentasjon for dette fra sertifiseringsorganet bør vedlegges søknaden.

- Låsen må ved behov kunne skjermes for avlesning/avtitting av dreieskive, display, tastatur eller tilsvarende.

- Kombinasjoner må minimum være sekssifret.

- Elektroniske kombinasjonslåser må ha sperrefunksjon som sperrer låsen i et antall minutter etter setting av et antall feilkoder.

- Elektroniske kombinasjonslåser bør vedlegges produsentens tekniske dokumentasjon for elektronisk design/sikkerhetsfunksjoner.

- For biometrisk lås behøves særlig utfyllende dokumentasjon om sikkerhetsfunksjoner mot manipulering.

- Kombinasjonslås der identifisering av bruker kun skjer ved inntasting av kode på tradisjonelt tastatur vil ikke bli gitt godkjenning som hovedlås for graderingene HEMMELIG og STRENGT HEMMELIG

Andre manipuleringssikrede kombinasjonslåser tidligere godkjent av Forsvarets overkommando/Sikkerhetsstaben tillates brukt på eksisterende installasjoner inntil videre, men den enkelte virksomhet anbefales å vurdere utskifting.

7.4.2 Lås # 2, tilleggslås

NSM tillater bruk av alle låser som er gitt godkjenning for KONFIDENSIELT som lås nummer 2.

Fortrinnsvis bør det benyttes en sikkerhetslås av tilholdertypen. Denne låskategorien har relativt god fysisk beskyttelse da den er montert på innsiden og i sin helhet beskyttet av dørens massivitet. Låsen bør være av omstillbar type da dette forenkler oppgaven ved tap av nøkkel eller mistanke om kompromittering. Dersom det ikke er mulig å installere en tilholderlås kan det benyttes en sylinderlås. Kun unntaksvis bør hengelås benyttes. Dersom det er ønskelig kan det også benyttes kombinasjonslås som lås nummer 2. Det bør da ikke benyttes samme kode på begge låsene.

7.5 Daglås og krav til rømning

Mange steder kan det være ønskelig med en tilleggslås til bruk på dagtid. Det mest hensiktsmessige vil normalt være en elektronisk lås i forbindelse med virksomhetens adgangskontrollsystem. Avhengig av omgivelsene kan slik avlåsning aksepteres brukt i forbindelse med kortere fravær. Forhold som bør vurderes er graden av kontroll i omliggende områder, tilstedeværelse av besøkende og personell uten sikkerhetsklarering, sikkerheten i adgangskontrollsystemet og mengde/gradering av den aktuelle informasjonen. Se også veiledningens kapittel om automatiske adgangskontrollanlegg.

Ved dårlig planløsning kan krav til sikker avlåsing mot innbrudd komme i konflikt med krav til rømning. Dersom kravene til sikker avlåsning ikke kan oppfylles er det vesentlig at en rømning medfører reaksjon som ved et innbrudd. Det vil blant annet si at brudd på nødnøkkelforsegling, bruk av rømningsbeslag eller automatisk opplåsing ved strømbrudd eller brannalarm også aktiverer innbruddsalarmanlegget. Det finnes et antall låsprodukter på markedet som i ulike kombinasjoner kan imøtekomme begge kravsett, og ved særlige behov kan NSM kontaktes for veiledning.

8 Dører

Hengsler representerer ofte et svakt punkt for angrep. Dører som slår utover bør derfor alltid sikres i bakkant. Bakkantsikringer fåes i flere varianter og består i et sett med bolter eller klør som holder dørens hengselside i inngrep med dørkarmen dersom hengslene kuttes.

Innfesting av dørkarm er også ofte et svakt punkt. Dersom karmen ikke er tilstrekkelig boltet fast eller avstivet, særlig i området rundt låsen, kan den enkelt bendes løs. Forskriften stiller ingen konkrete krav til ytterdører eller dører til beskyttet område eller til rom der det oppbevares BEGRENSET. Som et minimum bør det allikevel kontrolleres at hengsler, avstiving og innfesting av dørkarmen er av en slik kvalitet at døren ikke enkelt kan brekkes opp eller løsnes uten at det settes tydelige visuelle spor.

Branndører ser generelt solide ut, men kan ha svak konstruksjon rundt innfesting for låskasse og hengsler. Dersom det er påkrevet å benytte en branndør bør denne derfor være av innbruddsforsterket type samt forberedt for dørautomatikk. Det er verd å merke seg at en forsterkning i ettertid kan føre til at døren mister sin brannklassifisering. Blant annet gjelder dette ved boring i dørbladet for påsetting av ekstra lås, bakkantsikring, beslag og automatikk for åpning/lukking etc. Det bør derfor klarlegges på forhånd om det er behov for brannsikring slik at det kan anskaffes en kombinert brann- og sikkerhetsdør.

Dører til rom sikret for oppbevaring av KONFIDENSIELT skal være forsterket mot innbrudd. Som norm anbefales bruk av FG-godkjente sikkerhetsdører minimum klasse 2 etter standard NS-3170, eller klasse 3 etter standard EN 1627.

Rom for oppbevaring av HEMMELIG skal sikres som hvelv. Som norm benyttes her FG-godkjente hvelvdører minimum klasse 2 etter standard EN 1143-1. Sikkerhetsdører kan også benyttes dersom disse har FG-godkjenning minimum klasse 5 etter standard ENV 1627 eller tilsvarende. Dersom det er behov for å benytte dører som ikke innehar FG-godkjenning skal søknad om bruk fremmes NSM.

Det kan være behov for modifisering av dør eller reileverk for ettermontering av låser. I slike tilfeller er det avgjørende at arbeidet utføres av en kompetent håndverker. Forhold som avlastning av låsereiler, tilpassning til reileverk, innslags- og borsikringer bør vektlegges.

Dersom konstruksjonen av et sperret område ikke fullt ut svarer til basiskravene, men det er benyttet tilstrekkelig kompenserende tiltak, bør dørene være av minimum tilsvarende styrke som tilstøtende vegger. Det forutsettes at døren kan forsynes med godkjente låser for den aktuelle graderingen.

9 Elektronisk sikring

Som nevnt tidlig i denne veilederen har tidsforsinkende barrierer mindre verdi dersom de ikke kompletteres med muligheter for deteksjon av uvedkommende og inntrengere. Mangfoldet av produkter er stort, og det finnes utstyr som registrerer, varsler, overvåker og kontrollerer ulike slag funksjoner og hendelser. Nedenfor gis en kortfattet veiledning i bruken av elektroniske sikringsmidler og en beskrivelse av hvilke tiltak som anbefales og godkjennes for sikring av sikkerhetsgradert informasjon.

9.1 Adgangskontrollsystemer

Elektroniske systemer for adgangskontroll er utbredt og benyttes ved de fleste virksomheter. De forenkler endringer i interne tilgangsrettigheter og gir bedre muligheter for oversikt enn ved bruk av et

større antall mekaniske nøkler. Systemene anbefales brukt i de fleste tilfeller for kontrollert og beskyttet område, særlig der omfanget av fysiske nøkler er stort eller det er hyppig skifte av personell.

9.1.1 Anskaffelse

Et automatisk adgangskontrollanlegg er normalt oppbygget av en sentralenhet, leseenheter ved de ulike dørene og elektromekaniske låser. Det vanligste er online systemer der alle avleste "nøkler" godkjennes av sentralenheten før døren åpnes. Det finnes ulike typer med prinsipielle forskjeller. De vanligste er magnetkort, smartkort og berøringsfrie kort eller tags, gjerne i kombinasjon med bruk av PIN-kode. Systemer som benytter biometriske kjennetegn som fingeravtrykk, hånd- stemme- og øyegjenkjenning er ennå ikke særlig utbredt i det norske markedet. De prinsipielle forskjellene består i om en husket kode gir tilgang, om "nøkkelen" alene gir tilgang, eller om et biometrisk kjennetegn må presenteres før systemet gir tilgang. Adgangskontrollen kan også bestå av kombinasjoner av disse metodene.

De enkleste systemene benytter en husket kode. Disse har den ulempen at koden kan gies bort eller tilegnes av uvedkommende uten at dette registreres og mottiltak iverksettes. Andre systemer benytter eksempelvis magnetkort eller berøringsfrie tags. Disse har fremdeles den ulempen at de kan mistes eller stjeles, men dette blir da enklere oppdaget. Eventuelt kan de også lånes bort eller kopieres. Dersom man i stedet benytter biometriske kjennetegn er man noe sikrere på at det faktisk er rette person som gis adgang, alt avhengig av hvilket kjennetegn som benyttes. Kombinerer man kort, tag eller biometri med krav om presentasjon av en husket kode økes sikkerheten en del, men selv med kombinasjoner risikerer man at kort og kode kan lånes bort til eller tilegnes av andre. Det er viktig å være oppmerksom på at det er svakheter knyttet til alle teknologiene. Det er ingen metode som er 100% sikker. Særlig er kanskje troen på biometriens fortreffelighet overdrevet hos mange. Her er det blant annet en del ulemper knyttet til personvernet, og en dårlig løsning kan ved misbruk få store konsekvenser for den enkelte. Balansen mellom feilrate på gjenkjenning og avvisning kan også være en utfordring. Det vil også alltid være en andel personer som ikke ønsker eller kan presentere et gitt biometrisk kjennetegn. Hvilken variant eller kombinasjoner av koder, kort, tags eller biometri som skal brukes bør avgjøres på grunnlag av hva som er praktisk og hensiktsmessig for den enkelte virksomhet samt omfang og sensitivitet på verdier i området som skal kontrolleres.

Før man går til anskaffelse av et automatisk adgangskontrollanlegg anbefales det at man setter seg inn i ulike produsenters løsninger for å få et anlegg som er tilpasset det faktiske behovet. Sikkerheten kan raskt forringes ved at anlegget inneholder unødig funksjonalitet og derved blir uoversiktlig for administrator og operatører. NSM anbefaler at anskaffelse alltid gjøres hos en seriøs leverandør som også har et godt serviceapparat. Det bør ikke overlates til leverandøren alene å komme opp med et forslag til leveranse, men den sikkerhetsansvarlige og leverandøren bør gå sammen om å finne de mest hensiktsmessige løsningene.

Det bør kontraktsfestes at installasjonen i sin helhet gjøres i henhold til standard EN-50133. Dette vil bidra sterkt til at fallgruver unngås og at man får et sikkert anlegg som fungerer godt over lang tid.

9.1.2 Automatiske adgangskontrollanlegg for spesialrom

Det kan være aktuelt å benytte et elektronisk adgangskontrollsystem for avlåsning av sperret område eller andre spesialsikrede rom under kortere fravær på dagtid. Som nevnt i veilederens kapittel om låser avhenger dette blant annet av omgivelsene og sikkerheten i anlegget. For at en virksomhet selv skal kunne vurdere sikkerheten i et eksisterende adgangskontrollsystem har NSM utarbeidet en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Sjekklisten følger som vedlegg til denne veilederen.

I særlige tilfeller kan virksomheter ønske å benytte et automatisk adgangskontrollanlegg som erstatning for manuelle låser for samtale-/konferanserom eller spesialrom der det kreves godkjente låser. Et automatisk adgangskontrollanlegg vil kunne introdusere svakheter utover de som er tilstede ved bruk av en separat og unik lås. Blant annet er gjennomgang av rutiner og teknisk status på et adgangskontrollanlegg vesentlig mer komplisert og tidkrevende enn kontroll med én fysisk nøkkel. På den annen side kan et automatisk adgangskontrollanlegg tilføre muligheter for bedre loggfunksjoner.

Det vil imidlertid være vilkår knyttet til en eventuell godkjenning fra NSM i det enkelte tilfelle.

- Anlegget må i sin helhet være installert i henhold til standard EN 50133 "Access control systems for use in security applications". Dette innbefatter planlegging og design, de enkelte komponenter, kommunikasjon, installasjon og dokumentasjon. Aksesspunkter til de aktuelle områdene må være i klasse 3B.

- Det må foreligge instruks for drift og rutine for vedlikehold.

- Personell som gis adgang til sentralutrustning og kan programmere adgangsrettigheter skal være autorisert for dette av ansvarlig sjef. Antall autoriserte skal holdes på et minimum og ikke være andre enn det sikkerhetspersonell som også ellers ville hatt tilgang til nøkler til de aktuelle områdene.

- Nøkler til spesialrom skal ikke medbringes utenfor virksomhetens område. Dette prinsippet må også overføres til adgangskontrollsystemet, og det må derfor benyttes egne adgangskort som oppbevares i godkjent nøkkelskap i beskyttet område.

For at en godkjenning av et automatisk adgangskontrollanlegg skal kunne gis til dette formålet, vil NSM kreve utfyllende dokumentasjon i henhold til vilkårene over.

9.1.3 Registrering

Adgangskontrollsystemer skal registreres ved melding til Datatilsynet. Slik melding skal sendes senest 30 dager før oppstart; jf. Personopplysningsloven § 31. Personopplysningsloven med forskrifter gir videre regler om behandling av personopplysninger og bruk av loggfunksjoner i systemene. Særlig viktig er behandling av personopplysninger ved bruk av biometriske løsninger. For mer informasjon se www.datatilsynet.no.

9.2 Innbruddsalarmsystemer

Alarmsystemer benyttes ved de fleste virksomheter og kan være en rimelig erstatning for manuelt vakthold. Ved større eller særlig utsatte virksomheter som har døgnbasert vakthold vil de også utgjøre et verdifullt verktøy for øket kontroll.

9.2.1 Anskaffelse

Alarmsystemer består i grovt av sensorer, signalkabler, lokalt betjeningspanel, strømforsyning, sentralapparat og alarmoverføringslinjer. Sensorer finnes i mange varianter, både passive og aktive. De vanligste til bruk i innbruddsalarmsystemer er detektorer som registrerer temperaturforskjeller og bevegelse, glassbrudd og vibrasjoner/boring samt åpning av dører og vinduer. Ved valg og plassering av sensorer er det viktig å ta hensyn til de enkeltes dekningsområde for å unngå gliper i alarmsonen. En overlapping med kombinasjon av ulike typer sensorer kan og være å foretrekke. Hvilke sensorer som bør benyttes er avhengig konstruksjon og struktur på rommet / området som skal sikres og hvilke omgivelser det er i. Miljøfaktorer i form av eksempelvis lys, lyd, temperatur og vibrasjoner vil påvirke valget. Særlig utsatt for påvirkning og ustabile forhold er sensorer plassert utendørs.

Det er viktig å være oppmerksom på at det er svakheter knyttet til alle teknologier. Det er ingen sensor som er 100 % sikker, og det er av stor betydning med korrekt kalibrering og regelmessig vedlikehold for å sikre optimal ballanse mellom deteksjonsevne og fravær av feilalarmer.

Prinsipielt bør deteksjon forekomme i forkant av en tidsforsinkende fysisk barriere. Likeså bør deteksjon utfylles med mulighet for verifikasjon, for eksempel ved bruk av kompletterende sensorer eller kamera. Dette bør tillegges vekt da en alarm som ikke er verifisert sjelden fremkaller en adekvat reaksjon.

Før man går til anskaffelse av et alarmanlegg anbefales det at man setter seg inn i ulike produsenters løsninger for å få et anlegg som er tilpasset det faktiske behovet. Sikkerheten kan raskt forringes ved at anlegget inneholder unødig funksjonalitet og derved blir uoversiktlig for administrator og operatører.

NSM anbefaler at anskaffelse av alltid gjøres hos en seriøs leverandør som også har et godt serviceapparat. Det bør ikke overlates til leverandøren alene å komme opp med et forslag til leveranse, men den sikkerhetsansvarlige og leverandøren bør gå sammen om å finne de mest hensiktsmessige løsningene.

Det bør kontraktsfestes at installasjonen i sin helhet gjøres i henhold til standard EN-50131. Dette vil bidra sterkt til at fallgruver unngås og at man får et sikkert anlegg som fungerer godt over lang tid.

Den enkelte virksomhet er ansvarlig for å kontrollere at alle iverksatte sikringstiltak fungerer etter sin hensikt. For å lette denne egenkontrollen med alarmsystemer har NSM utarbeidet en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Sjekklisten følger som vedlegg til denne veilederen.

9.2.2 Alarmlegging av særlig viktige rom

For sikring av rom der det lagres informasjon gradert STRENGT HEMMELIG kreves bruk av alarmanlegg dersom det ikke er kontinuerlig manuelt vakthold. Forskriften fastslår at ”*Et elektronisk sikringsanlegg skal som minimum dekke arealet rundt hvelvet og hvelvdøren og termineres i bemannet vakt der det skal foreligge plan for reaksjon. Beregnet maksimum reaksjonstid skal være mindre enn beregnet innbruddstid*”. Alarmanlegget skal som et minimum dekke arealet rundt hvelvet. Det er altså ikke tilstrekkelig med eksempelvis magnetkontakt på døren eller en bevegelsesdetektor på innsiden som varsler om at innbrudd har funnet sted. Hensikten er at det tidlig skal detekteres og reageres på forsøk på inntrengning eller uønsket tilstedeværelse i hvelvets / rommets umiddelbare nærhet. Behovene for oppbygging av anlegget vil variere alt etter virksomhetstype og omgivelser, og NSM stiller ingen absolutte minimumskrav til kvalitet eller hvilke komponenter anlegget skal inneholde. Anlegget bør imidlertid i størst mulig grad tilfredsstille kravene til grad 3 etter standard EN 50131; (FG-godkjenning grad 3).

Virksomheten må kunne dokumentere at anlegget er tilstrekkelig dimensjonert og at det fungerer etter sin hensikt. Det vises her til forskrift om sikkerhetsadministrasjon kapittel 4 om risikohåndtering og sikkerhetsrevisjon.

9.3 Kameraer

Kameraer kan anvendes til å holde ett eller flere områder under generelt oppsyn, verifisere en alarm, eller identifisere personell før en dør åpnes etc. Det er imidlertid viktig å merke seg at tradisjonelle kameraer alene sjelden gir noen god evne til sanntids deteksjon av uønsket tilstedeværelse. En operatør vil normalt ikke vil være i stand til å holde konsentrasjonen oppe over et lengre tidsrom. Kombinert med at det gjerne er flere monitorer å forholde seg til, at det må svitsjes mellom ulike kameraposisjoner eller endog parallelle arbeidsoppgaver som skal utføres, vil man derfor ikke oppnå kontinuerlig overvåking. Konstellasjonen kamera/operatør har derfor en begrenset verdi og er ikke særlig anvendbar til kontroll i inntrengningshemmende forstand. Dersom man kombinerer bruk av kameraer med andre tiltak oppnår man derimot flere fordeler.

9.3.1 Anskaffelse

Den enkleste kombinasjonen er gjerne kamera med videoopptaksutstyr som kan brukes til å verifisere et hendelsesforløp i ettertid. Gitt tilstrekkelig billedkvalitet kan dette være et nyttig hjelpemiddel i etterforskningsøyemed, men det har i hovedsak kun en begrenset avskrekkende effekt og vil ikke fremkalle reaksjon mot selve inntrengningen. Kameraer kommer best til sin rett dersom de også kombineres med et innbruddsalarmanlegg. Systemet bør da kobles slik at operatøren automatisk får displayet området hvor en detektor har gitt varsel. Dette har den fordelen at et alarmsignal kan verifiseres i forkant av en eventuell utrykning og at vaktpersonalet derved vet mer om hvilken trussel de står overfor.

Nyere kameraovervåkingssystemer kan ha funksjoner som deteksjon av bevegelse eller persongjenkjenning m.m. Koblet til digitale lagringsmedia kan disse ta opp store mengder video, enten kontinuerlig, i faste intervaller, eller med automatisk lagring av billeddata fra tidsrommet før en alarm

fant sted. Kombinerer man så kameraovervåking med innbruddsalarm og adgangskontroll har man et komplett system for elektronisk sikring. Et slikt skreddersydd system kan være verdifullt for større virksomheter eller lokaliteter med stort sikringsbehov.

Før man går til anskaffelse av ett eller flere kameraer anbefales det at man setter seg godt inn i hvilket behov man faktisk har og hva det enkelte kamera skal brukes til. Altfor ofte ser vi eksempler på at det er valgt feil kameratype, feil linse, plasseringen var ikke optimal, det var for dårlig lys osv. Dette resulterer i at video og bilder slett ikke er brukbare til det behovet man ser i ettertid. For at en virksomhet lettere skal kunne planlegge og kontrollere sitt kameraanlegg har NSM laget en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Sjekklisten følger som vedlegg til denne veilederen.

NSM anbefaler at anskaffelse av et kameraanlegg alltid gjøres hos en seriøs leverandør som også har et godt serviceapparat. Det bør ikke overlates til leverandøren alene å komme opp med et forslag til leveranse, men den sikkerhetsansvarlige og leverandøren bør gå sammen om å finne de mest hensiktsmessige løsningene.

Det bør kontraktsfestes at installasjonen i sin helhet gjøres i henhold til standard EN-50132. Dette vil bidra sterkt til at fallgruver unngås og at man får et sikkert anlegg som fungerer godt over lang tid.

9.3.2 Registrering

Kameraovervåkning skal meldes til Datatilsynet før oppstart, jf Personopplysningsloven § 37. Melding skal sendes senest 30 dager før oppstart. Nærmere bestemmelser om denne type overvåkning er gitt i Personopplysningsloven kapittel VII og personopplysningsforskriften kapittel 8. For mer informasjon se– www.datatilsynet.no .

9.4 Bruk av elektroniske sikringsanlegg

NSM vil minne om betydningen av at anleggenes funksjoner tilpasses det faktiske behovet slik at det ikke blir unødig komplisert og uoversiktlig. Dette kan fort gi en kunstig sikkerhetsfølelse. Sikkerhet er ikke et fysisk produkt, og viktigere enn tekniske finesser er rutinene rundt og menneskene som skal håndtere anlegget.

Et elektronisk sikringsanlegg er ikke vedlikeholdsfritt. Dette er et forhold som erfaringsmessig tillegges for liten vekt. Gode rutiner for regelmessig kontroll, justering og testing iht en serviceavtale er avgjørende for anleggets funksjon over tid og for å kunne oppdage eventuelle svakheter. Vi anbefaler også at denne veilederens kontrollskjemaer benyttes for egenkontroll, gjerne i forbindelse med årlig sikkerhetsrevisjon.

10 Plombering

I visse situasjoner vil plombering være en verdifull tilleggssikring av sikkerhetsgradert informasjon og materiale. Plombering skal sikre at uautorisert åpning vil bli oppdaget. Forskriften inneholder egne bestemmelser om emballering og plombering ved forsendelser av sikkerhetsgradert materiale både med og uten kurér. De konkrete kravene fastslås særskilt i §§ 4-20, 8-4, 8-8 og 8-17. Bestemmelsene angir overordnede krav til emballasje, personell og håndtering av plomberingsutstyr. Imidlertid er det mange typer plomberingsutstyr tilgjengelig på markedet med ulike kvaliteter og bruksområder, og forskriften er ikke konkret på hva slags utstyr som skal brukes i enhver sammenheng. For at virksomhetene selv skal kunne vurdere kvaliteten på de ulike teknikkene samt lettere ta stilling til egne behov, har NSM laget en oversikt over de mest prinsipielle forskjellene.

10.1 Emballasje

Emballasje skal være tilstrekkelig solid slik at utilsiktet brekkasje ikke skal oppstå. Den må derfor være motstandsdyktig mot både riving, støt, press og fuktighet. Sammenføyninger skal heller ikke kunne

åpnes uten at det setter tydelige spor og emballasjen ødelegges, eksempelvis ved å løsne limte skjøter ved bruk av damp eller kjemikalier.

Emballasjen må også være ugjennomsiktig. Dette fordi ingen skal kunne få innsyn uten å måtte ødelegge forpakningen. Det må heller ikke være mulig å fukte emballasjen med vann eller kjemikalier slik at den slipper gjennom lys. I visse tilfeller kan det også være aktuelt å bruke materialer som skjermer mot gjennomlysning med teknisk apparatur, eksempelvis røntgen eller ultralyd med mer.

10.2 Plomberingsutstyr

Et nøkkelord ved all bruk av forseglingsutstyr er tillit. Det må være stor grad av tiltro til at plombering er foretatt av rett personell og at det faktisk er korrekt plombe som kontrolleres av mottaker. For å bidra til dette skal alt forseglingsutstyr oppbevares minst som for informasjon gradert KONFIDENSIELT, og bare særskilt utpekt og sikkerhetsklarert personell skal ha tilgang til utstyret. Brukte plomber bør ikke kastes, men makuleres.

Det er en rekke produsenter og leverandører, og plomber kommer i mange utførelser. Det kan eksempelvis være enkle klips, plaststrips eller metallwire med pregede numre, tradisjonell forseglingstape, eller også mer avanserte systemer som gir tilnærmet full teknisk tillit. NSM anbefaler at virksomheten vurderer ulike produkttyper opp mot eget behov. Nedenfor er listet noen spørsmål som bør besvares før valget tas. De ulike egenskaper ved plombemateriale kan sjelden vurderes med ja- og nei- svar, det vil som regel være grader av kvalitet og aksept.

Hvor lett er det å **manipulere** (dirke) plomben?
- Hva kreves av kompetanse og utstyr?

Hvor lett er det å **reparere** en brutt plombe?
- Hva kreves av kompetanse og utstyr?

Hvor lett er det å **erstatte** eller **kopiere** en brutt plombe?
- Er plomben kommersielt lett tilgjengelig?
- Preges plomben av en leverandør eller med avsenders proprietære utstyr?
- Er pregeutstyr lett kommersielt tilgjengelig eller enkelt å lage?

Hvor høy er terskelen for god **kontroll** av at plomben er intakt / ekte?
- Kunnskap og rutiner i praksis hos mottaker.

Hvordan er **brukervennlighet**?
- Administrasjon, id-merking, påsetting, kontroll, avklipping, registrering, rapportering.

Er motstand mot utilsiktet **brekkasje** god nok for den tiltenkte forsendelsesmetode?

11 Dokumentasjon

Forskrift om informasjonssikkerhet og denne veilederen sier noe om hvordan fysiske sikringstiltak skal eller kan utformes. Det er ulike måter å sette sammen det ønskede sett av tiltak for deteksjon, tidsforsinkende barrierer og reaksjonsmuligheter på. Hvordan tiltakene så bør dokumenteres avhenger i stor grad av virksomhetens størrelse eller kompleksitet og eventuelt om noe krever godkjenning, eksempelvis kryptoinstallasjoner, spesialrom eller informasjonssystemer. Noen tiltak er grunnleggende for virksomheten og dokumentasjon hører naturlig hjemme i grunnlagsdokument for sikkerhet eller andre sentrale dokumenter, mens andre tiltak bør dokumenteres særskilt for en enkelt godkjenning. Det bør tilstrebes at dokumentasjonen er så konsis som mulig og at tiltak kun dokumenteres ett sted.

Grunnlagsdokument for sikkerhet skal inneholde inndelingen i fysiske områder ved virksomheten, jf forskrift om sikkerhetsadministrasjon § 3-3. En hensiktsmessig måte å dokumentere inndelingen på er vanligvis ved bruk av en bygningstegning, områdeskisse eller lignende. Inndelingen skal angi hvor den graderte informasjonen tillates behandlet og oppbevart, samt hvilket graderingsnivå som er det høyest tillatte for det enkelte området. En beskrivelse av vaktordninger kan også inngå i grunnlagsdokumentet.

Virksomhetens sikkerhetsinstruks og sentrale sikkerhetsdokumentasjon bør inneholde oversikt over oppbevaringsenheter, adgangsbestemmelser for de ulike områder, instruks for nøkkelhåndtering, kontrollrutiner og annet som er av gjennomgående karakter. Eksempelvis vil det være

uhensiktsmessig å måtte dokumentere virksomhetens elektroniske og bygningstekniske sikringstiltak eksplisitt for hvert informasjonssystem som skal godkjennes.

Søknader om godkjenning av informasjonssystemer må inneholde beskrivelser av fysiske sikringstiltak som er relevant for den lokale installasjonen. Dersom sentrale sikkerhetsdokumenter er utarbeidet med innhold som beskrevet over vil det ofte være tilstrekkelig å vise til disse. Tilleggsinformasjon om særskilt sikring av spesielle rom og utstyr, og særlig containere, vil det være naturlig at beskrives for den enkelte godkjenning. Det skal blant annet vurderes motstandsevne mot inntrengning med bruk av fysisk makt og tradisjonelt verktøy samt med fordekte metoder. Kort listet kan innholdet derfor bli noe slikt:

- Materialer i tak, gulv og vegger.
- Dørtyper, forsterkning, beslag, hengsling, låstyper og kobling til låsemekanisme.
- Kabel- og ventilasjonsgjennomføringer og sikring av disse.
- Sammenføyninger (sveiset, boltet, skrudd, poppet, limt etc).
- Vinduer, type, hengsling, innfesting, karm, gitter.
- Andre forhold av betydning for inntrengningstid eller deteksjonssannsynlighet f.eks. bruk av safer, vakter, alarmanlegg.

Søknader om godkjenninger bør inneholde gode nærbilder av det som beskrives slik at særlig mulighetene for fordekt inntrengning kan bedømmes.

Dokumentasjon som behøves i forbindelse med godkjenning av kryptorom er beskrevet i egen veileder tilgjengelig under ”regelverk” på www.nsm.stat.no.

12 Dokumenthistorie

2004-09-01	Første utgave
2006-05-16	Utvidet elektronisk sikring
2006-11-09	Oppdatert med mindre justeringer
2008-07-14	Utvidet nettverkskomponenter og elektronisk sikring m/ vedlegg 1, 2 og 3
2010-03-16	Oppdatert nøkkelskap og låser samt mindre justeringer
2011-05-25	Ny fil grunnet teknisk feil. Kosmetiske endringer.
2011-08-19	Oppdatert K-skap
2013-06-12	Oppdatert låser.
2014-06-10	Oppdatert låser og noen mindre justeringer
2014-19-12	Godkjent serverskap for gradering HEMMELIG
2015-04-08	Godkjent serverskap for gradering HEMMELIG

Kontrollskjema for automatiske adgangskontrollanlegg

Vedlegg #1 - til veiledning i Fysisk sikring mot ulovlig inntrengning.

For at en virksomhet selv skal kunne vurdere sikkerheten i et eksisterende adgangskontrollsystem har NSM utarbeidet en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Svarene bør vektlegges i henhold til foreslått vektingstall:

Kategori 1: Spørsmål av avgjørende betydning. Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør anses som en "showstopper" uavhengig av hva andre kontrollpunkt gir til svar.

Kategori 2: Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør vurderes samlet med andre svar. Vurder sårbarhet og eventuelle kompenserende tiltak.

Kontrollskjemaet bør ses i sammenheng med veilederens kapittel om elektronisk sikring.

Sentralenhet

Hovedenhet for styring av anlegget og programmering av adgangsrettigheter.

Spørsmål	Er enheten plassert innenfor minimum beskyttet område?
Hvorfor	Plassering innenfor beskyttet område innebærer at personell med permanent adgang innehar en sikkerhetsklarering. Tiltaket reduserer risikoen for innsidetrusler mot anlegget.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enheten sikret mot uautorisert fysisk tilgang?
Hvorfor	Sentralenheten kan manipuleres. Den bør derfor være plassert i et rom eller et skap som er godt sikret mot fordekt inntrengning.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Spørsmål	Er enheten utstyrt med sabotasjealarm?
Hvorfor	Sentralenheten kan manipuleres. Det bør være mulighet for deteksjon av åpning av kabinett samt logging av slik hendelse.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Benyttes autentiseringskode for programmering, lesing og sletting av logger?
Hvorfor	Kun særskilt utpekt personell bør gis tilgang til å programmere anlegget. Bruk av brukernavn og passord / tilsvarende utgjør en ytterligere buffer utover fysisk tilgang til enheten. Bruk av autentiseringskode vil også ansvarliggjøre de autoriserte i større grad.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Aktiviseres en alarm ved x antall feilkoder?
Hvorfor	Forsøk på uautorisert ”logisk tilgang” til sentralenheten bør oppdages.
Måleenhet	Ja – Nei
Akseptabel verdi	Ja
Vekting	2

Interfaces og koblingsbokser

Andre enheter enn sentralenhet og lesere.

Spørsmål	Er enhetene plassert på sikker side?
Hvorfor	Det kan være muligheter for å manipulere åpningssignaler ved å foreta omkoblinger i enhetene. En plassering på ”sikreste side” reduserer antallet personer som vil ha fysisk tilgang til enheten.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enhetene utstyrt med sabotasjealarm?
Hvorfor	Det kan være muligheter for å manipulere åpningssignaler ved å foreta omkoblinger i enhetene. Det bør være mulighet for deteksjon av åpning av dører/deksler samt logging av slik hendelse.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Er det muligheter for programmering eller betjeningsoppgaver i enheten?
Hvorfor	Dersom det er mulig å utføre oppgaver som det kreves autorisasjon for, bør enheten sikres tilsvarende som sentralenheten.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Leseenheter

Enheter der brukeren presenterer koder og tokens. Eksempelvis tastaturer og kortlesere.

Spørsmål	Har leseenheten tampersikring?
Hvorfor	Leseenheter kan manipuleres til å kompromittere inntastede koder og informasjon på adgangskort og andre tokens. Forsøk på manipulering bør oppdages.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Har leseren andre funksjoner enn avlesing av kode / token?
Hvorfor	Dersom enheten inneholder logikk som tar beslutning om å gi adgang, må kvaliteten på tampersikringen vies stor vekt. Dersom enheten inneholder releer eller lignende som gir styringssignaler til låsen må enheten være svært godt fysisk sikret.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Nei
Vekting	2

Låsen

Alle låser og sluttstykker som styres av anlegget.

Spørsmål	Er låsen av FG-godkjent type?
Hvorfor	Låser er generelt et sårbart og utsatt angrepspunkt. En FG-godkjenning innebærer at produktet er testet og holder en viss minimumsstandard mtp motstandsdyktighet mot manipulering og brekkasje. Både låskasse, sluttstykke, evt sylinder og sikkerhetsskilt, samt montering må kontrolleres.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Er det mulig å komme til kablingen fra utsiden?
Hvorfor	Låsen opererer når den får spenning fra anlegget. Dersom det er mulig å komme til ledningene kan man åpne låsen ved koble disse om eller påsette spenning fra en ekstern strømkilde.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I svært liten grad
Vekting	1

Spørsmål	Er døren utstyrt med åpen/lukket/låst statusføler?
Hvorfor	Dører kan bli stående åpne eller ulåst. Dette kan skyldes dårlig vedlikehold eller villet handling / menneskelig svikt. Det er en fordel om anlegget registrerer status slik at forholdet kan utbedres raskt.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Kabling

Alle ledninger og koblingspunkter som forbinder de ulike enhetene i anlegget.

Spørsmål	Er kabler tilstrekkelig sikret eller skjult?
Hvorfor	Signaler kan manipuleres og anlegget kan saboteres dersom uvedkommende får fysisk tilgang til kabler. Alle ledninger bør derfor legges skjult. Dersom de må legges lett tilgjengelig eller synlig må det være på ”sikreste side”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Strømtilførsel

Alle kurser som anleggets komponenter er avhengig av for uforstyrret drift.

Spørsmål	Er anlegget utstyrt med batteribackup eller nødstrøm fra aggregat?
Hvorfor	Ved strømbrudd vil dører enten holdes permanent låst eller permanent ulåst avhengig av konfigurasjon. Begge tilstander medfører problemer i en periode hvor driftspersonell og vakter også vil ha andre utfordringer og tidspress.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er alle enheter utstyrt med nødstrømtilførsel?
Hvorfor	Et adgangskontrollanlegg kan være forsynt med strøm fra flere kurser. Anlegget kan også være avhengig av andre installasjoner for å fungere – eksempelvis nettverk for signaloverføring.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er alarm ved strømbrudd eller feil som medfører åpning av dører koblet til alarmanlegget?
Hvorfor	Strømbrudd eller feil i adgangskontrollanlegget kan være forårsaket av en villet handling med ulovlig inntrengning som formål. Forholdet bør undersøkes umiddelbart.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Administrasjon

Konfigurasjonskontroll, driftsrutiner og instrukser med mer.

Spørsmål	Er anlegget innmeldt til Datatilsynet?
Hvorfor	Adgangskontrollsystemer skal registreres ved melding til Datatilsynet; jf. Personopplysningsloven § 31. Personopplysningsloven med forskrifter gir videre regler om behandling av personopplysninger og bruk av loggfunksjoner i anlegget.
Måleenhet	Ja – Nei – Vet ikke.
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er det tatt bevisst stilling til hvorvidt dører skal låses eller låses opp ved feil i adgangskontrollanlegget eller ved brann?
Hvorfor	Hvorvidt dører skal låses eller låses opp er i første rekke en avveining mellom behov for security og krav til uforstyrret inn- og utpassering samt rømningsmuligheter. Det bør ligge en argumentasjon til grunn som understøtter valget. Argumentasjonen kan variere mellom ulike områder og aksesspunkter.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er det lik sikkerhetsklassifisering på alle aksesspunkter til det enkelte område?
Hvorfor	Et område kan ha flere innpasseringsveier. Krav til gjenkjenning og adgang bør være lik for alle dører til et område. Gjenkjenningsklasser: 0: Trykknapp 1: Kode 2: Token eller biometri 3: Token eller biometri + kode Adgangsklasser: A: Ikke tidsbestemt (adgang 24/7) B: Tidsbestemt + logg Ba: Tidsbestemt uten logg
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Tillates klasse 0 exit utenom arbeidstid?
Hvorfor	Besøkende / uvedkommende kan skjule seg og bli værende alene igjen i lokalet etter normal arbeidstid. Klasse 0 åpning fra innsiden etter normal arbeidstid bør unngås da disse således kan forlate området udetektert.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Nei
Vekting	2

Spørsmål	Finnes rutiner for handling ved feil i anlegget?
Hvorfor	Tekniske alarmer og registrering av uønsket status på dører og låser er et varsel om at anlegget ikke fungerer etter sin hensikt, eventuelt kan det være et tegn på forsøk på ulovlig inntrengning. Likeså registrering av bruk av feil koder og uautoriserte tokens. Alle varsler bør derfor undersøkes umiddelbart, og tekniske forhold bør utbedres så snart som praktisk mulig.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Vil åpning av nødutganger medføre alarm?
Hvorfor	Nødutganger skal fungere som klasse 0 exit. Nødutganger benyttes også erfaringsmessig som ”røykedør” av personalet og kan glemmes i åpen/ulåst tilstand. Nødutganger bør bare kunne benyttes til rømning. Annen bruk bør registreres og alarm verifiseres.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Kan logger slettes av flere?
Hvorfor	Inn- og utpasseringer, tekniske alarmer og hendelser samt programmering som er foretatt bør logges. Det kan være mulighet for å slette loggene og det bør ikke kunne reises tvil om hvem som har gjort det. Adgang til dette bør om mulig begrenses til 1 person. Eventuelt bør det være en logg for hendelser på sentralapparatet som er ”uslettelig”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Spørsmål	Finnes det en rutine for produksjon av tokens og programmering av adgangsrettigheter?
Hvorfor	Adgangsrettigheter skal gis i henhold til et tjenstlig behov. Det må være klart hvem som beslutter at adgang skal gis og hvordan dette skal dokumenteres.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Finnes det en rutine for sletting eller endring av adgangsrettigheter?
Hvorfor	Adgangsrettigheter skal opphøre når det tjenstlige behovet ikke lenger er tilstede. Dersom en ansatt slutter skal adgangsrettigheter slettes. Dersom en ansatt skifter stilling, eller det tjenstlige behovet for adgang av andre årsaker endres, skal behovet vurderes på nytt.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Kontrolleres tokens og adgangsdatabasen regelmessig?
Hvorfor	For å ha god kontroll på låsesystemer skal opptelling av nøkler utføres regelmessig. Dette gjelder alle typer nøkler, også adgangskort m.v.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Kontrollskjema for innbruddsalarmanlegg

Vedlegg #2 - til veiledning i Fysisk sikring mot ulovlig inntrengning.

For at en virksomhet selv skal kunne vurdere sikkerheten i et eksisterende innbruddsalarmanlegg har NSM utarbeidet en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Svarene bør vektlegges i henhold til foreslått vektingstall:

Kategori 1: Spørsmål av avgjørende betydning. Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør anses som en "showstopper" uavhengig av hva andre kontrollpunkt gir til svar.

Kategori 2: Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør vurderes samlet med andre svar. Vurder sårbarhet og eventuelle kompenserende tiltak.

Kontrollskjemaet bør ses i sammenheng med veilederens kapittel om elektronisk sikring.

Sentralapparat

Hovedenhet for programmering, styring og sending av alarmer.

Spørsmål	Er enheten plassert innenfor minimum beskyttet område?
Hvorfor	Plassering innenfor beskyttet område innebærer at personell med permanent adgang innehar en sikkerhetsklarering. Tiltaket reduserer risikoen for innsidetrusler mot anlegget.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enheten sikret mot uautorisert fysisk tilgang?
Hvorfor	Sentralenheten kan manipuleres. Den bør derfor være plassert i et rom eller et skap som er godt sikret mot fordekt inntrengning.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Spørsmål	Er enheten utstyrt med sabotasjealarm?
Hvorfor	Sentralenheten kan manipuleres. Det bør være mulighet for deteksjon av åpning av kabinett samt logging av slik hendelse.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Benyttes autentiseringskode for programmering, lesing og sletting av logger?
Hvorfor	Kun særskilt utpekt personell bør gis tilgang til å programmere anlegget. Bruk av brukernavn og passord / tilsvarende utgjør en ytterligere buffer utover fysisk tilgang til enheten. Bruk av autentiseringskode vil også ansvarliggjøre de autoriserte i større grad.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Aktiviseres en alarm ved x antall feilkoder?
Hvorfor	Forsøk på uautorisert ”logisk tilgang” til sentralenheten bør oppdages.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Interfaces og koblingsbokser

Andre enheter enn sentralenhet og sensorer.

Spørsmål	Er enhetene plassert på sikker side?
Hvorfor	Det kan være muligheter for å manipulere alarmsignaler ved å foreta omkoblinger i enhetene. En plassering på ”sikreste side” reduserer antallet personer som vil ha fysisk tilgang til enheten.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enhetene utstyrt med sabotasjealarm?
Hvorfor	Det kan være muligheter for å manipulere alarmsignaler ved å foreta omkoblinger i enhetene. Det bør være mulighet for deteksjon av åpning av dører/deksler samt logging av slik hendelse.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Er det muligheter for programmering eller betjeningsoppgaver i enheten?
Hvorfor	Dersom det er mulig å utføre oppgaver som det kreves autorisasjon for, bør enheten sikres tilsvarende som sentralenheten.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Spørsmål	Er betjeningsenheten skjermet mot innsyn?
Hvorfor	Når kode for frakobling av alarmanlegget tastes kan dette observeres av uvedkommende. Det er derfor viktig at betjeningsenheten er plassert slik at avtitting ikke er sannsynlig. Det bør i størst mulig grad også tas hensyn til at avlesning kan foretas med tekniske hjelpemidler på lang avstand.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Sensorer

Alle typer følere og detektorer. Eksempelvis magnetkontakter og bevegelsesdetektorer.

Spørsmål	Har sensorene tampersikring?
Hvorfor	Sensorer kan frakobles, tildekkes, flyttes eller på annen måte settes ut av drift når alarmanlegget ikke er tilkoblet. Forsøk på manipulering bør oppdages.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er sensorenes dekningsområde hindret?
Hvorfor	Interiør som for eksempel reoler eller gardiner kan ha blitt flyttet slik at dekningsområdet ikke lenger er som forutsatt da anlegget ble prosjektert.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Nei
Vekting	2

Spørsmål	Er det gliper i alarmsonen?
Hvorfor	Det kan være installert for få sensorer i forhold til områdets størrelse eller antallet adkomstveier. Alle inntrengningsveier bør være dekket av minst en sensor.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Nei
Vekting	2

Spørsmål	Er sensorene plassert på rett side av barrieren?
Hvorfor	Prinsipielt bør deteksjon forekomme i forkant av en tidsforsinkende barriere. Dersom sensoren er på ”innsiden”, detekteres inntrengningen for sent. Deteksjon på ”innsiden” kan likevel være del av et verifikasjonstiltak.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Kabling

Alle ledninger og koblingspunkter som forbinder de ulike enhetene i anlegget.

Spørsmål	Er kabler tilstrekkelig sikret eller skjult?
Hvorfor	Signaler kan manipuleres og anlegget kan saboteres dersom uvedkommende får fysisk tilgang til kabler. Alle ledninger bør derfor legges skjult. Dersom de må legges lett tilgjengelig eller synlig må det være på ”sikreste side”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Strømtilførsel

Alle kurser som anleggets komponenter er avhengig av for uforstyrret drift.

Spørsmål	Er anlegget utstyrt med batteribackup eller nødstrøm fra aggregat?
Hvorfor	Ved strømbrudd vil alarmanlegget slutte å fungere og ingen alarmer vil sendes. Sabotasje av strømtilførsel kan også være en metode en motstander vil bruke forut for en inntrengning.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er alle enheter utstyrt med nødstrømtilførsel?
Hvorfor	Et alarmanlegg kan være forsynt med strøm fra flere kurser. Anlegget kan også være avhengig av andre installasjoner for å fungere – eksempelvis modem og IP-nett for alarmoverføring.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Administrasjon

Driftsrutiner og instrukser med mer.

Spørsmål	Er det etablert rutiner for vedlikehold og test av anlegget?
Hvorfor	Alarmanlegg er ikke vedlikeholdsfrie. Sensorers dekningsområde og følsomhet kan variere og reduseres over tid. Backupbatterienes effekt, linjer for overføring av alarmer og avhengigheter til andre systemer kan endres uten at dette oppdages i daglig drift. Regelmessige rutiner bør minimum omfatte følsomhetstest av alle sensorer, kontroll av batterikapasitet, alarmoverføring og reaksjon.
Måleenhet	Ja – Nei – Vet ikke.
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Finnes rutiner for handling ved feil i anlegget?
Hvorfor	Tekniske alarmer og feil på sensorer eller alarmlinjer er et varsel om at anlegget ikke fungerer etter sin hensikt, eventuelt kan det være et tegn på forsøk på sabotasje eller inntrengning. Alle varsler bør derfor undersøkes umiddelbart, og tekniske forhold bør utbedres så snart som praktisk mulig.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Kan logger slettes av flere?
Hvorfor	Til- og frakobling, tekniske alarmer og hendelser samt programmering som er foretatt bør logges. Det kan være mulighet for å slette loggene og det bør ikke kunne reises tvil om hvem som har gjort det. Adgang til dette bør om mulig begrenses til 1 person. Eventuelt bør det være en logg for hendelser på sentralapparatet som er ”uslettelig”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Spørsmål	Finnes det en rutine for endring av koder?
Hvorfor	Koden for frakobling av alarmanlegget kan tilegnes av uvedkommende. Den må derfor skiftes regelmessig og ved mistanke om kompromittering. Risikoen øker med antallet personer som kjenner koden og intervallet mellom endringer. Koden bør også skiftes når noen med kjennskap til den slutter eller ikke har behov for den lenger.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Kontrollskjema for kameraovervåkingsanlegg

Vedlegg #3 - til veiledning i Fysisk sikring mot ulovlig inntrengning.

For at en virksomhet selv skal kunne vurdere sikkerheten i et eksisterende kameraovervåkingsanlegg har NSM utarbeidet en sjekkliste. Listen inneholder en del sentrale spørsmål med en kort forklaring om hvorfor spørsmålet bør stilles, samt en indikasjon om hva som vil være et akseptabelt svar. Svarene bør vektlegges i henhold til foreslått vektingstall:

Kategori 1: Spørsmål av avgjørende betydning. Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør anses som en "showstopper" uavhengig av hva andre kontrollpunkt gir til svar.

Kategori 2: Mangelfull implementering av sikkerhetstiltak iht. dette kontrollpunktet bør vurderes samlet med andre svar. Vurder sårbarhet og eventuelle kompenserende tiltak.

Kontrollskjemaet bør ses i sammenheng med veilederens kapittel om elektronisk sikring.

Sentralutrustning

Hovedenhet for styring og lagring av video.

Spørsmål	Er enheten plassert innenfor minimum beskyttet område?
Hvorfor	Plassering innenfor beskyttet område innebærer at personell med permanent adgang innehar en sikkerhetsklarering. Tiltaket reduserer risikoen for innsidetrusler mot anlegget.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enheten sikret mot uautorisert fysisk tilgang?
Hvorfor	Sentralenheten kan manipuleres eller saboteres. Den bør derfor være plassert i et rom eller et skap som er godt sikret mot fordekt inntrengning.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Spørsmål	Er enheten utstyrt med sabotasjealarm?
Hvorfor	Sentralenheten kan manipuleres. Det bør være mulighet for deteksjon av åpning av kabinett samt logging av slik hendelse.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Benyttes autentiseringskode for programmering, avspilling og sletting av video?
Hvorfor	Kun særskilt utpekt personell bør gis tilgang til å programmere, spille av og slette video. Bruk av brukernavn og passord / tilsvarende utgjør en ytterligere buffer utover fysisk tilgang til enheten. Bruk av autentiseringskode vil også ansvarliggjøre de autoriserte i større grad.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Aktiviseres en alarm ved x antall feilkoder?
Hvorfor	Forsøk på uautorisert ”logisk tilgang” til sentralenheten bør oppdages.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Interfaces og koblingsbokser

Andre enheter enn sentralenhet og kameraer.

Spørsmål	Er enhetene plassert på sikker side?
Hvorfor	Det kan være muligheter for å manipulere videosignaler ved å foreta omkoblinger i enhetene. En plassering på ”sikreste side” reduserer antallet personer som vil ha fysisk tilgang til enheten.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Er enhetene utstyrt med sabotasjealarm?
Hvorfor	Det kan være muligheter for å manipulere videosignaler ved å foreta omkoblinger i enhetene. Det bør være mulighet for deteksjon av åpning av dører/deksler samt logging av slik hendelse.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Spørsmål	Er det muligheter for programmering eller betjeningsoppgaver i enheten?
Hvorfor	Dersom det er mulig å utføre oppgaver som det kreves autorisasjon for, bør enheten sikres tilsvarende som sentralenheten.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Kameraer

Spørsmål	Er kameraene lett tilgjengelige?
Hvorfor	Kameraer kan frakobles, tildekkes, dreies eller på annen måte settes ut av drift. De bør derfor være montert slik at de er vanskelig tilgjengelige, eventuelt være beskyttet med vandalsikret hus.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2

Spørsmål	Er kameraenes dekningsområde hindret?
Hvorfor	Interiør, eksteriør eller vegetasjon kan ha endret seg slik at dekningsområdet ikke lenger er som forutsatt da anlegget ble prosjektert.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Nei
Vekting	2

Spørsmål	Er kameraet av riktig type?
Hvorfor	Ofte viser deg seg at video og bilder ikke egner seg når noe skjer. Det er derfor viktig at kamera og linse er tilpasset et definert formål, alt fra ansiktsgjenkjenning til registrering av aktivitet i et større område. Flere kameraer kan være nødvendig for å dekke ulike behov i ett område.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	1

Spørsmål	Er kameraene plassert riktig?
Hvorfor	Kameraer bør monteres slik at de i minst mulig grad påvirkes av ujevne eller skiftende lys- og solforhold. Eventuelt bør det suppleres med tilleggsbelysning eller solskjerm. Kameraer som benyttes til verifikasjon av alarmer bør minimum dekke sensorens alarmsone.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Kabling

Alle ledninger og koblingspunkter som forbinder de ulike enhetene i kamerasystemet.

Spørsmål	Er kabler tilstrekkelig sikret eller skjult?
Hvorfor	Signaler kan manipuleres og anlegget kan saboteres dersom uvedkommende får fysisk tilgang til kabler. Alle ledninger bør derfor legges skjult. Dersom de må legges lett tilgjengelig eller synlig må det være på ”sikreste side”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I meget stor grad – i stor grad
Vekting	2

Strømtilførsel

Alle kurser som anleggets komponenter er avhengig av for uforstyrret drift.

Spørsmål	Er anlegget utstyrt med batteribackup eller nødstrøm fra aggregat?
Hvorfor	Ved strømbrudd vil verifisering av alarmer vanskeliggjøres, overvåking og opptak av bilder og video avbrytes. Sabotasje av strømtilførsel kan også være en metode en motstander vil bruke forut for en inntrengning.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er alle enheter utstyrt med nødstrømtilførsel?
Hvorfor	Et overvåkingsanlegg kan være forsynt med strøm fra flere kurser. Anlegget kan også være avhengig av andre installasjoner for å fungere – eksempelvis nettverksutstyr for videooverføring.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Administrasjon

Driftsrutiner og instrukser med mer.

Spørsmål	Er anlegget innmeldt til Datatilsynet?
Hvorfor	Kameraovervåkingsanlegg skal registreres ved melding til Datatilsynet; jf. Personopplysningsloven § 37. Personopplysningsloven med forskrifter gir videre regler om behandling av personopplysninger og bruk av opptaksmateriale.
Måleenhet	Ja – Nei – Vet ikke.
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Er det etablert rutiner for vedlikehold av anlegget?
Hvorfor	Kameraovervåkingsanlegg er ikke vedlikeholdsfrie. Kvalitet på opptaksutstyr kan reduseres over tid og kameraers lysfølsomhet og fokus kan endres. Backupbatterienes effekt og avhengigheter til andre systemer kan endres uten at dette oppdages i daglig drift. Regelmessige rutiner bør minimum omfatte kontroll av opptakskvalitet og reserve strømtilførsel.
Måleenhet	Ja – Nei – Vet ikke.
Akseptabel verdi	Ja
Vekting	2

Spørsmål	Finnes rutiner for handling ved feil i anlegget?
Hvorfor	Tekniske alarmer og feil på bildeoverføring er et varsel om at anlegget ikke fungerer etter sin hensikt, eventuelt kan det være et tegn på forsøk på sabotasje eller inntrengning. Alle varsler bør derfor undersøkes umiddelbart, og tekniske forhold bør utbedres så snart som praktisk mulig.
Måleenhet	Ja – Nei – Vet ikke
Akseptabel verdi	Ja
Vekting	1

Spørsmål	Kan videoopptak og logger slettes av flere?
Hvorfor	Lagring og sletting av data, tekniske alarmer og hendelser samt programmering som er foretatt bør logges. Det kan være mulighet for å slette video og logger og det bør ikke kunne reises tvil om hvem som har gjort det. Adgang til dette bør om mulig begrenses til 1 person. Eventuelt bør det være en logg for hendelser på sentralapparatet som er ”uslettelig”.
Måleenhet	I meget stor grad – i stor grad – i liten grad – i svært liten grad – vet ikke
Akseptabel verdi	I liten grad – i svært liten grad
Vekting	2