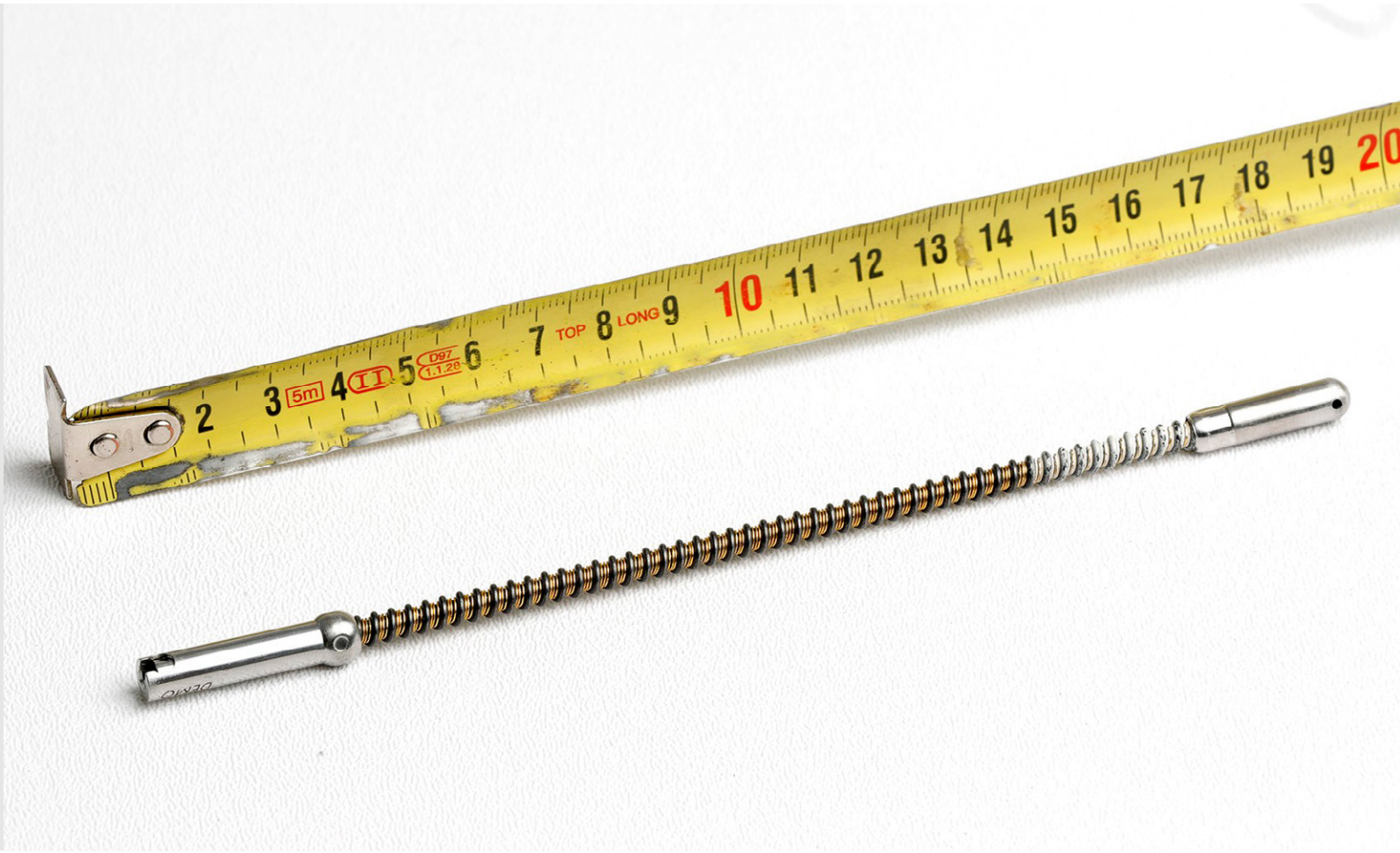
STUK OPASTAA / TOUKOKUU 2023



Säteilylähteiden turvajärjestelyt – opas käytännön toteutukseen

Turvajärjestelyjen tasot A ja B

Kannen kuva: Jukka Mykkänen

ISBN 978-952-309-561-8 (pdf)
ISSN 1799-9472

Johdanto

Säteilyn käyttöä koskevat säteilyturvallisuustoimet eivät aina huomioi riittävästi sitä mahdollisuutta, että säteilylähde voi joutua lainvastaisen toiminnan kohteeksi. Säteilylähdettä voidaan esimerkiksi vahingoittaa tietoisesti tai käyttää vahingoittamistarkoituksessa. Tällaisten tapausten varalta säteilyturvallisuustoimenpiteitä on tarpeen täydentää turvajärjestelyillä.

Tässä oppaassa kuvataan käytännön turvajärjestelyjä, joilla voidaan saavuttaa Säteilyturvakeskuksen määräyksessä esitetyn mukainen turvallisuustaso. **Määräyksen velvoittava teksti on esitetty lihavoituna kappaleen alussa**. Muuten oppaassa esitetyt kohdat ovat ohjeistavia, toiminnanharjoittajalle tueksi suunnittelua ja toteutusta varten. Erityisesti uusia tiloja suunniteltaessa on syytä harkita standardien mukaisia ratkaisuja ja turvajärjestelyihin perehtyneen konsultoinnin käyttöä.

Tämän oppaan luvut 2–3 keskittyvät tarkentamaan turvajärjestelyistä annettua STUKin määräystä STUK S/9/2021. Ohjeistava teksti pyrkii kuvaamaan STUKin näkemystä siitä, miten vaatimuksia tulisi – tai ei tulisi toteuttaa.

Sisällys

1 Määritelmät

Turvajärjestelyt (Security measures):
Toimenpiteet, joilla pyritään havaitsemaan ja ehkäisemään säteilylähteeseen kohdistuva lainvastainen toiminta (esimerkiksi varkaus, sabotointi tai laiton siirtäminen taikka luvaton sisään tunkeutuminen näitä lähteitä sisältäviin laitoksiin tai tiloihin). Näihin toimenpiteisiin kuuluvat myös vastatoimenpiteet lainvastaisen teon tapahduttua.

Lainvastainen toiminta:
Tahallinen toiminta tai toimenpide, jonka tarkoituksena on säteilyn käytön turvallisuuden tai säteilylähteen koskemattomuuden vaarantaminen tai muun välittömän tai välillisen uhan aiheuttaminen säteilyturvallisuudelle taikka säteilylähteeseen kohdistuvan tuottamuksellisen vahingon aiheuttaminen.

Liikuteltava säteilylaite:
Säteilylaite, joka on tarkoitettu tarvittaessa siirrettäväksi käyttöpaikasta toiseen joko kantamalla tai muutoin helposti esimerkiksi erillisellä kärryllä tai laitteessa itsessään olevien pyörien avulla.

Turvajärjestelyjen osa-alueet:
Lainvastaisen toiminnan ennaltaehkäisy (deterrence), havaitseminen (detection), viivyttäminen (delay) ja vaste (response). Vasteeseen kuuluvat lainvastaisen toiminnan pysäyttäminen, tilanteen hallintaan saattaminen sekä seurausten estäminen ja rajoittaminen.

Käyttöpaikka (turvajärjestelyvaatimusten osalta):
Yksittäinen huone tai muu vastaavaa rajattu tila. Yhdessä rakennuksessa voi olla useita erillisiä säteilyn käyttöpaikkoja tai säteilylähdevarastoja.

Säteilylähteen välittömässä läheisyydessä oleva este:
Esimerkiksi käyttöpaikan tai säteilylähdevaraston ovi on lukittu tai säteilylähdettä säilytetään erillisessä lukitussa kaapissa.

Säteilylähteen käyttöpaikan tai varastotilan ulkopuolella oleva este:
Esimerkiksi käyttöpaikka tai varasto sijaitsee rakennuksessa, jonka ulko-ovet on lukittu, tai lukitulla aidatulla alueella.

Kulunvalvonta:

Pääsyn rajoittaminen alueelle tai tilaan sekä alueella liikkuvien valvonta.

Kulunvalvontaan voivat kuulua esimerkiksi sähköiset ovilukitukset, kulkuoikeuksien määrittely työntekijäkohtaisesti ja henkilön tunnistus (koodi, avain, biometrinen tunniste tai vastaava). Jos sähköistä kulunvalvontaa ei ole, kulunvalvonta voidaan järjestää esimerkiksi siten, että paikan avain luovutetaan vain nimetyille henkilöille kuittausta vastaan ja vain siksi ajaksi, kun tehtävien hoidon kannalta on tarpeen. Käyttötilanteessa kuluvalvonta voidaan hoitaa siten, että käyttöhenkilöstö on jatkuvasti läsnä ja huolehtii siitä, että edellä mainitut kulunvalvonnan tavoitteet toteutuvat.

Säteilylaitteen omaan suojukseen tai toimintaan liittyvä rakenne, joka toimii rakenteellisena esteenä:

Tällaisia laitteita voivat olla esimerkiksi

- teollisuuslaitoksessa kiinteästi asennettu radiometrinen mittalaite
- laite, jonka siirtäminen vaatisi sellaista siirto- ja kuljetuskalustoa, jonka käyttö kyseisessä kohteessa merkittävästi vaikeuttaa ja hidastaa lähteen haltuunottoa
- säteilyä sähköisesti tuottava laite on varustettu käynnistysavaimella tai -koodilla tai on muulla tavoin vain käyttöhenkilöstön käynnistettävissä.

Insider-henkilö:

Henkilö, jolla on pääsy säteilylähteeseen tai sitä koskevaan tietoon.

2 Turvajärjestelyjen taso B

4 § Turvajärjestelyjen taso B

Turvajärjestelyt on toteutettava tason B mukaisesti, jos:

1) **umpi- tai avolähteen aktiivisuus on suurempi tai yhtä suuri kuin STUKin määräyksen S/9/2021 liitteessä olevassa taulukossa esitetty aktiivisuus; tai**

2) **samassa käyttö- tai säilytyspaikassa olevilla umpi- ja avolähteillä toteutuu ehto**

   $\sum_n \frac{A_n}{R_n} \geq 1$ **, missä**

   A_n on radionuklidia n olevan yksittäisen umpi- tai avolähteen aktiivisuus.

   Avolähteen tapauksessa A_n on radionuklidia n sisältävän avolähteen suurin toiminnassa käytettävä aktiivisuus.

   R_n on radionuklidin n liitteessä olevassa taulukossa esitetty aktiivisuus;

3) **kysymyksessä on teollisuuskuvaustoimintaan tarkoitettu verkkovirralla toimiva, liikuteltava, sähköisesti säteilyä tuottava laite.**

Kauppakamarin yritysturvallisuuskyselyn perusteella useimmat yritykset käyttävät murtohälytystä tai rikosilmoitinjärjestelmää (76 %). Toiseksi yleisin tapa suojata omaisuutta on henkilöstön koulutus (70 %). Kolmanneksi eniten mainintoja sai vartiointi (64 %). Kulunvalvontaa, valvontajärjestelmien toimivuuden säännöllistä testausta, videovalvontaa ja tuotanto-, toimisto- ja tuotekehitystilojen eriyttämistä käyttää kuusi kymmenestä yrityksestä. (Kauppakamari, Yritysten rikosturvallisuus 2017)

2.1 Rakenteelliset esteet

8 § Rakenteelliset esteet turvajärjestelyjen tasolla B

Turvajärjestelyjen tasolla B säteilylähteet on suojattava vähintään kahdella rakenteellisella esteellä. Vähintään toisen rakenteellisista esteistä on oltava joko säteilylaitteessa itsessään tai laitteen välittömässä läheisyydessä.

Rakenteelliset esteet voidaan korvata henkilöstön läsnäololla. Jos rakenteelliset esteet korvataan henkilöstön läsnäololla, henkilöstöllä on oltava mahdollisuus viestiä lainvastaisesta toiminnasta tai sen epäilystä välittömästi.

Rakenteellisilla esteillä tarkoitetaan sellaisia fyysisiä rakenteita, joilla vaikeutetaan ja hidastetaan pääsyä säteilylähteen luokse ja siten pyritään ehkäisemään lähteen luvaton haltuunotto tai lähteeseen kohdistuva vahingonteko.

Rakenteellisia esteitä voivat olla tilanteen mukaan seinät, katto, lattia, ovet, ikkunat ja aitaukset. Ovien, ikkunoiden ja muiden aukkojen on oltava riittävästi murtosuojattuja, jotta ne voivat toimia rakenteellisina esteinä. Rakenteellisten esteiden tulee olla tasapainoisia, esim. oven, seinien ja ikkunoiden suojauskyvyn tulee vastata toisiaan.

Rakenteellista estettä koskevat yksityiskohdat selvitetään turvajärjestelysuunnitelmassa. Fyysisten rakenteiden lisäksi rakenteellinen este voi olla myös laitteen ominaisuus, joka vaikeuttaa ja hidastaa sen väärinkäyttöä tai luvatonta haltuunottoa, esimerkiksi

- kiinteästi asennettu radiometrinen mittalaite
- laitteen siirtoa vaikeuttava suuri massa
- vain käyttäjien hallussa oleva röntgenlaitteen käynnistysavain tai -koodi.

Säteilylaitteen välittömässä läheisyydessä oleva rakenteellinen este voi olla esimerkiksi

- laitteen käyttö- tai säilytyspaikkana oleva lukittu huone
- säteilylähteen säilytykseen käytettävä riittävän varma kaappi, esimerkiksi turvakaappi tai kassakaappi

Rakenteellisen esteen korvaaminen henkilöstön läsnäololla voi tulla kyseeseen esimerkiksi silloin, kun kuljetettavia säteilylähteitä käytetään kentällä eikä fyysisiä rakenteita ole käytettävissä.

Myös kiinteästi asennetuilla säteilylähteillä riittäisi, että käyttöhenkilöstö on läsnä ja käyttämässä säteilylähdettä tai voi koko ajan valvoa säteilylähdettä, vaikka sitä ei aktiivisesti käytettäisikään.

Seuraavaksi esitellään ratkaisuvaihtoehtoja rakenteellisiksi ratkaisuiksi.

2.1.1 Säteilylähde

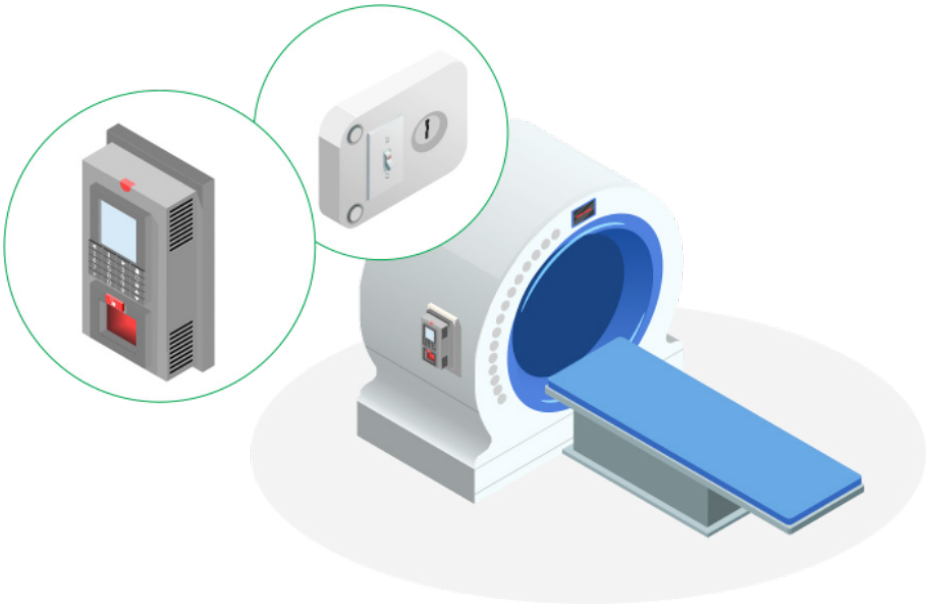
Rakenteellisena esteenä voi toimia kiinteästi asennettu umpilähde itsessään, kun umpilähde ei ole irrotettavissa ilman käsityökaluja tai siirrettävissä ilman apuvälineitä.

Säteilylaitteen omaan suojukseen tai toimintaan liittyvä rakenne voi toimia rakenteellisena esteenä. Tällainen rakenne voi olla esimerkiksi raskas suojus, jonka siirtäminen vaatisi sellaista siirto- ja kuljetuskalustoa, jonka käyttö kyseisessä kohteessa merkittävästi vaikeuttaa ja hidastaa lähteen haltuunottoa.

Umpilähteen raskas suojus ei kuitenkaan voi toimia rakenteellisena esteenä, jos sitä säilytetään siirtämistä auttavan alustan, kuten trukkilavan tai lavetin päällä. Tällöin laite tulisi esimerkiksi ankkuroida kiinni rakenteisiin.

KUVA 1. Helposti liikuteltavia säteilylaitteita valmiina lähtöön.

Mikäli kyseessä on röntgenlaite, rakenteellisena esteenä voi toimia avain tai koodi, joka on vain käyttöhenkilöllä. Mikäli avain tai koodi ei ole yksilöllinen (laitteen voi käynnistää millä tahansa avaimella), se ei välttämättä voi toimia rakenteellisena esteenä.



KUVA 2. Säteilylaitteen rakenteellisena esteenä voi toimia yksilöllinen koodi tai avain.

2.1.2 Säilytyskaappi

Säilytyskaapin tulee olla tarpeeksi vahva, jotta sitä ei voi murtaa tai irrottaa ilman käsityökaluja.

Säilytyskaapin tulee olla tarpeeksi vahva ja asianmukaisesti lukittu. Säilytyskaappi kannattaa ankkuroida rakenteisiin. Uutta säilytyskaappia hankittaessa kannattaa harkita standardien mukaisia kaappeja.

Finanssiala ry:n mukaan

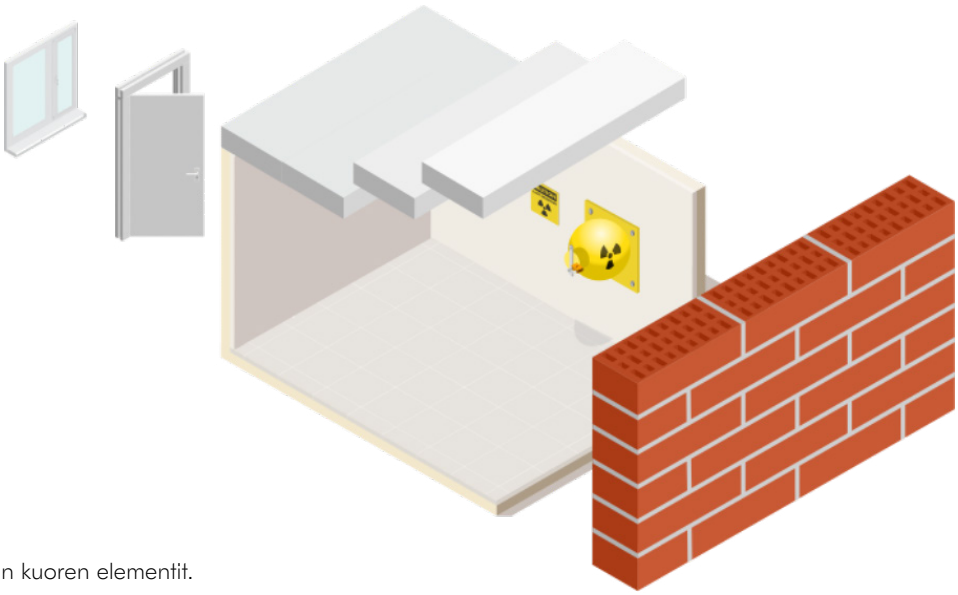
- säilytyskaappi on standardin SFS-EN 1143-1 mukaan vähintään luokkaan 1 murtotestattu kassakaappi
- kassakaapilla tarkoitetaan arvosäilytysyksikköä, joka on testattu ja hyväksytty standardin SFS-EN 1143-1 mukaan ja tästä osoituksena on sertifiointilaitoksen myöntämä todistus ja valmistajan asentama kyltti kassakaapin oven sisäpuolella.

2.1.3 Tilan kuori

Aluetta rajaavat rakenteet muodostavat kokonaisuuden, joka tarjoaa riskeihin nähden riittävän suojan asiattoman pääsyn estämiseksi.

Rakenteiden tulee olla lujuudeltaan ja rakennustavaltaan sellaisia, että tilaan tunkeutuminen ei ole mahdollista ilman työkaluilla tapahtuvaa rakenteiden rikkomista. Jos kiinteistöllä on useita käyttäjiä, ulkokuoren vaatimukset koskevat käyttö- ja varastotilaa.

Heikompaa rakennetta voi täydentää muilla turvajärjestelyillä, esimerkiksi parantamalla lukitusta tai asentamalla kalterit vahvistamaan ikkunan murtosuojausta.



KUVA 3. Tilan kuoren elementit.

Seinärakenteiden tulee olla betonia, terästä, tiiltä tai vahvaa puuta. Seinärakenteet ovat lähtökohtaisesti riittävät, mikäli ne eivät ole murrettavissa ilman työkaluja.

Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta.

Katto- ja lattiarakenteet ovat lähtökohtaisesti riittävät, mikäli ne eivät ole murrettavissa ilman työkaluja.

Puutteellisia rakenteita tulee vahvistaa.

Turvajärjestelysuunnitelmassa voidaan tarkentaa, mitä materiaalia seinärakenteet ovat.

2.1.4 Ikkunat

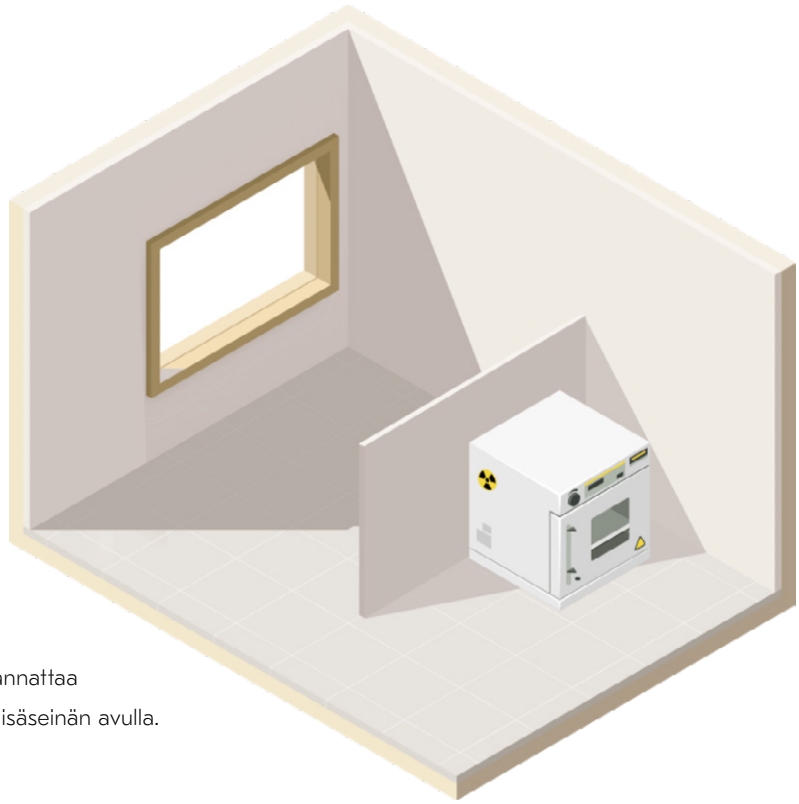
Ikkunoiden lasi tulee kiinnittää ja ikkunat sulkea siten, ettei niitä voi irrottaa tai avata ulkopuolelta rikkomatta.

Mikäli käyttö- tai säilytyspaikassa on kattoikkunoita, niitä suositellaan vahvistettavan.

Ikkunoiden suojausta voidaan parantaa esimerkiksi

- vahvistamalla alle 4 metrin korkeudella olevat ikkunat murronsuojalasilla tai -kalvolla, kaltereilla tai teräsristikolla
- suosimalla iskunkestävää lasia (SFS-EN 356 / P4A) ikkunoita hankittaessa tai uusittaessa.

Näköyhteys ulkoa säteilylähteeseen on syytä estää esimerkiksi keveän lisäseinän tai sermin avulla, sijoittamalla laite sopivaan paikkaan tai sumentamalla ikkuna näkösuojateippauksen avulla.



KUVA 4. Tarpeen tullen säteilylähde kannattaa piilottaa sivullisilta katseilta esimerkiksi lisäseinän avulla.

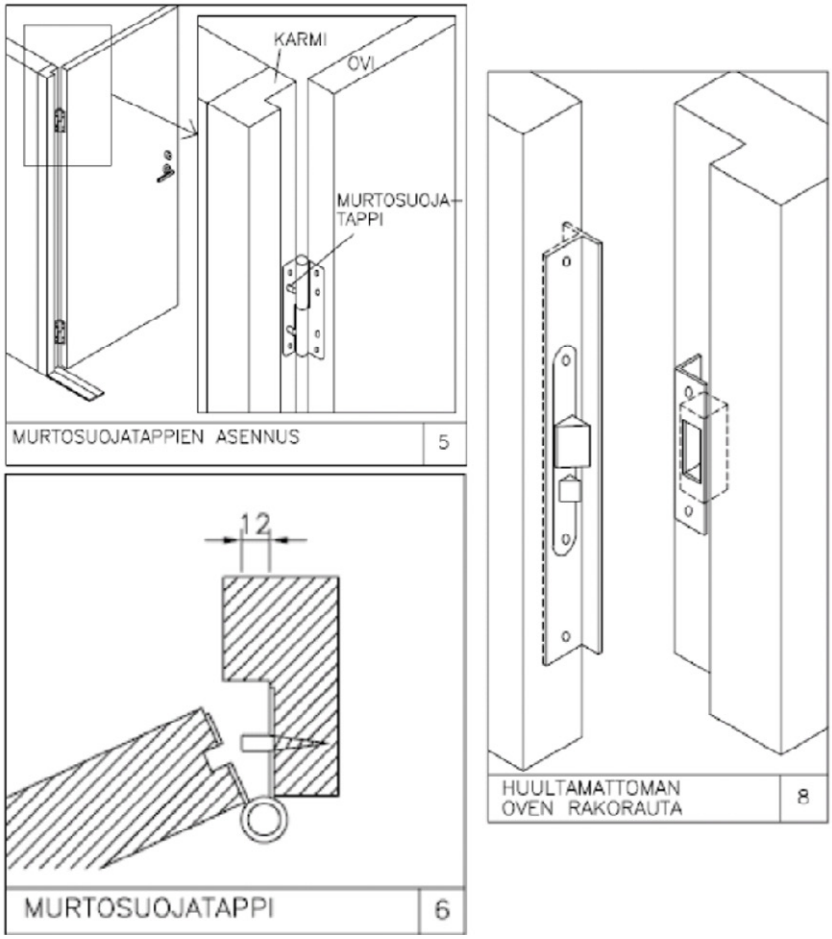
2.1.5 Ovet

Oven rakenteen tulee olla lujuudeltaan vähintään seinärakennetta vastaava. Mikäli ovessa on ikkuna, sen lujuus ei ole välttämättä riittävä. Ikkunaa voi vahvistaa kalterein tai murtosuojakalvolla.

Uusia ovia hankittaessa kannattaa harkita SFS EN 1627 luokka 3:n murronkestoluokan vaatimuksen täyttävää ratkaisua.

Ovien suojausta voidaan parantaa seuraavasti:

- Karmirakenteen on estettävä kiinnitysruuvien sahaaminen ulkoapäin.
- Saranoihin asennetaan murtosuojatapit.
- Oven ja karmin välys on lukkosivulla max. 5 mm.
- Huultamattoman oven käyttölukko suojataan rakoraudalla.



KUVA 5. Rakenteellinen murtosuojaus. Kuvat Finanssiala ry.

Huomioi, että halliovet ovat usein heikosti murtosuojattuja ja saattavat vaatia lisävahvistusta. Halliovien lukitukseen tulee kiinnittää erityistä huomiota.

2.1.6 Lukitus

Ovissa tulee olla käyttölukko eli kiinteästi oveen asennettava lukko vastalevyineen. Oven tulee olla lukittuna, kun tilassa ei työskennellä, jotta lukitus voidaan laskea rakenteelliseksi esteeksi.

Suojausta voidaan parantaa varmuuslukolla.

Ovien avaimiin suositellaan vähintään lukkoseppätasoa. Lukkoseppätaso on Suomessa yleisesti käytössä oleva avainturvallisuustaso, jonka mukaan lisäavaimen voi teettää vain lukkovalmistajan valtuuttamassa liikkeessä avainkortilla.

2.1.7 Aitaus

Aitaukseen suositellaan metalliverkkoaitaa, jonka korkeus on vähintään 2,4 m. Huomioi porttien lukitus työajan ulkopuolella ja sisäänkäyntien kulunvalvonta.

2.2 Pääsyn rajoittaminen säteilylähteiden käyttö- ja säilytyspaikkaan

7 § Toimet turvajärjestelyjen tasolla B

Turvajärjestelyjen tasolla B on toteutettava 6 §:ssä määrätyt järjestelyt ja niitä on täydennettävä tässä pykälässä määrätyllä tavalla.

6 § Toimet turvajärjestelyjen tasolla C

Pääsy säteilylähteiden käyttö- ja säilytyspaikkaan on rajoitettava vain niihin henkilöihin, joiden pääsyyn on säteilylähteistä tai käyttö- ja säilytyspaikasta huolehtimisesta johtuva perusteltu syy.

9 § Kulunvalvonta ja hälytysjärjestelmä turvajärjestelyjen tasolla B

Pääsy säteilylähteiden käyttö- ja säilytyspaikkaan on rajoitettava henkilöihin, joille on työn laatu ja luonne huomioiden annettu riittävät ohjeet ja opastus turvajärjestelyistä ja joilla on säteilylähteistä tai käyttö- ja säilytyspaikasta huolehtimisesta johtuva perusteltu syy pääsyyn.

Näitä henkilöitä ovat esimerkiksi säteilylähteitä käyttävät ja huoltavat tai käyttö- tai säilytyspaikasta huolehtivat henkilöt sekä vartiointihenkilöstö. Pääsy säteilylähteiden säilytyspaikkaan on selkeämmin rajattavissa vain tarpeellisiin henkilöihin, mikäli paikka on varattu pelkästään säteilylähteille.

Pääsyoikeuksista pidetään kirjaa, niitä tarkastetaan ja päivitetään säännöllisesti ja tarvittaessa. Pääsyoikeuksien tarkistaminen tulee kyseeseen esimerkiksi työtehtävien muuttuessa ja oikeuksien poistaminen työsuhteen päättyessä.

Pääsyä käyttö- ja säilytyspaikkaan voidaan rajoittaa esimerkiksi lukituksen ja kulunvalvonnan keinoin.

KUVA 6. Jos kulkuoikeudet eivät riitä avaamaan ovea, syttyy siitä merkiksi punainen valo.

Turvajärjestelysuunnitelmassa on hyvä selvittää, miten pääsyoikeuksia hallinnoidaan, pääsyoikeuksiin liittyvät vastuut sekä velvollisuudet.

2.3 Kulunvalvonta

9 § Kulunvalvonta ja hälytysjärjestelmä turvajärjestelyjen tasolla B

Turvajärjestelyjen tasolla B käyttö- ja säilytyspaikkaan on oltava kulunvalvonta.

Kulunvalvonnalla rajoitetaan pääsyä tietylle alueelle tai tilaan. Kulunvalvonnan tavoitteena on

- valvoa alueella liikkuvia
- estää asiattomien pääsy alueelle tai tilaan (esimerkiksi yleinen kulunvalvonta rakennuksen sisäänkäynnin yhteydessä)
- rajata pääsy valvottavalle alueelle tai tilaan vain niihin organisaation henkilöihin, joiden on päästävä sinne työtehtäviensä vuoksi.

Kulunvalvontaan voivat kuulua esimerkiksi sähköiset ovilukitukset, kulkuoikeuksien määrittely työntekijäkohtaisesti ja henkilön tunnistus (koodi, avain, biometrinen tunniste tai vastaava).

Kulunvalvontajärjestelmä ei ole rakenteellinen este.

2.3.1 Käyttö- ja säilytyspaikka

Säteilylähteiden käyttö- ja säilytyspaikkaan pääsevillä käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin tiloihin, tietoverkkoihin, tietoihin ja järjestelmiin.

Kulunvalvontaa voidaan toteuttaa ja parantaa seuraavilla ratkaisuilla:

- Käyttö- ja pääsyoikeudet myöntää ja niitä hallinnoi nimetty vastuuhenkilö.
- Käyttö- ja pääsyoikeuden haltijoista on lista.
- Käyttö- ja pääsyoikeuksien käsittely ja myöntäminen on ohjeistettu.
- Käyttö- ja pääsyoikeudet tarkistetaan säännöllisesti.
- Kulunvalvontajärjestelmä on hyvä kahdentaa ja akkuvarmentaa.

KUVA 7. Esimerkki kulunvanvalvontajärjestelmästä.

Kulunvalvonnan toteutus sekä käyttö- ja pääsyoikeuksien hallinnointi ja tarkastuksen toteutus kuvataan turvajärjestelysuunnitelmassa

2.3.2 Avaintenhallinta

Avainten hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu. Avainten hallintaan on nimetty vastuuhenkilö organisaatiossa ja hänellä on luettelo jaetuista ja hallussaan olevista avaimista sekä alueen lukostokaavio ja avainkortti.

Mikäli säteilylähteen luo pääsee yleisavaimella, on syytä selvittää yleisavaimia hallitsevat tahot. On myös selvitettävä aiheuttaako yleisavaimen käyttö hälytyksen.

Kulkuoikeudet tulee tarkistaa säännöllisesti ja tarvittaessa, jotta säteilylähteen luokse pääsevät vain asianomaiset henkilöt.

Avaintenhallinnassa on huomioitu perinteiset avaimet, sähköiset kulkuoikeudet sekä säilytyskaappien avaimet.

Avaintenhallinnan käytännöt kuvataan turvajärjestelysuunnitelmassa.

2.4 Säteilylähteiden käyttö- ja säilytyspaikan hälytysjärjestelmä

9 § Kulunvalvonta ja hälytysjärjestelmä turvajärjestelyjen tasolla B

Käyttö- ja säilytyspaikka, jossa säteilylähde voi olla valvomattomana, on oltava etävalvotun hälytysjärjestelmän piirissä. Hälytyksen on ohjauduttava automaattisesti paikkaan, josta hälytyksen varmistaminen voidaan aloittaa välittömästi.

Paikka, johon hälytyksen on ohjauduttava voi olla esimerkiksi vartiointiliike tai yrityksen työntekijä, kunhan hälytyksen varmentaminen voidaan aloittaa heti.

KUVA 8. Hälytyksen ohjautuminen matkapuhelimeen ja hälytyskeskukseen.

Valvottavia kohteita ovat esimerkiksi itse säteilylähde, ovet, ikkuna ja tila, jossa säteilylähde sijaitsee. Kohdevalvontaa kannattaa suunnitella riskiarvioinnin perusteella. Hälytysjärjestelmän tehokkaassa toteutuksessa voi hyödyntää esimerkiksi liiketunnistimia ja erilaisia ilmaisimia.

Liiketunnistimet

Liiketunnistimet hyödyntävät tyypillisesti infrapunatekniikkaa havaitsemaan normaalista poikkeavaa liikettä. Liiketunnistimen voi asentaa esimerkiksi säteilylähteiden käyttö- tai säilytyspaikkaan valvomaan luvatonta liikehdintää työajan ulkopuolella.

Ikkunoiden ja ovien ilmaisimet

Ikkunoihin ja oviin on saatavilla esimerkiksi tärinäilmaisimia tai lasinrikkoilmaisimia, joiden avulla murtautuminen voidaan havaita jo varhaisessa vaiheessa.

2.5 Suunnitelma turvajärjestelyistä

11 § Suunnitelma turvajärjestelyistä

Turvajärjestelyjen tasolla A ja B laadittavaan turvajärjestelyjä koskevaan suunnitelmaan pitää sisältää ainakin:

1) toiminnanharjoittajan nimi, säteilyn käyttöä koskevan turvallisuusluvan numero ja suunnitelman laatimis- tai julkaisupäivämäärä;

2) turvajärjestelyjen eri osapuolten välinen vastuunjako, luettelo vastuuhenkilöistä ja heidän tehtävistään;

3) säteilylähteiden käyttötarkoitus, luettelo turvajärjestelyjä koskevista säteilylähteistä ja umpilähteiden radionuklidi ja aktiivisuus tai avolähteiden suurin toiminnassa käytetty aktiivisuus;

4) kuvaus säteilylähteiden käyttö- ja säilytyspaikan sijainnista, turvajärjestelyjen tasosta, rakenteellisista esteistä, kulunvalvonnasta ja hälytysjärjestelmistä sekä kuva, johon on merkitty ainakin:
   a) säteilylähteiden sijainti;
   b) rakenteelliset esteet;
   c) kulunvalvontajärjestelmät;
   d) hälytysjärjestelmät;

5) ohjeet tai viittaukset ohjeisiin, jotka koskevat:
   a) säteilylähteiden säännöllisiä tarkistuksia;
   b) toimintaa ja viestintää poikkeavissa tapahtumissa;
   c) suunnitelman turvajärjestelyistä ja turvajärjestelyjen ajan tasalla pitämistä;
   d) turvajärjestelyasiakirjojen käsittelyä ja säilyttämistä.

Edellä on esitelty vähimmäisvaatimus turvajärjestelysuunnitelman sisällöstä. Suunnitelman laatimiseksi ja täydentämiseksi kannattaa ottaa huomioon seuraavaksi esitetyt tarkennukset:

1 Toiminnanharjoittajan nimi, säteilyn käyttöä koskevan turvallisuusluvan numero ja suunnitelman laatimis- tai julkaisupäivämäärä
   - Selvitä suunnitelman tai sen osien luottamuksellisuutta koskeva merkintä tässä kohdassa. Miten suunnitelman tietoturvallisuudesta on huolehdittu?

2 Turvajärjestelyjen eri osapuolten välinen vastuunjako, luettelo vastuuhenkilöistä ja heidän tehtävistään
   - Selvitä vastuuhenkilöiden pätevyydet ja koulutus.
   - Selvitä kiinteistön omistajan ja rakennuksen muiden käyttäjien osallisuus turvajärjestelyissä.
   - Selvitä myös esimerkiksi vartiointiliikkeiden tai muiden vastaavien alihankkijoiden osallisuus vastuunjaossa.

3 Säteilylähteiden käyttötarkoitus, luettelo turvajärjestelyjä koskevista säteilylähteistä ja umpilähteiden radionuklidi ja aktiivisuus tai avolähteiden suurin toiminnassa käytetty aktiivisuus

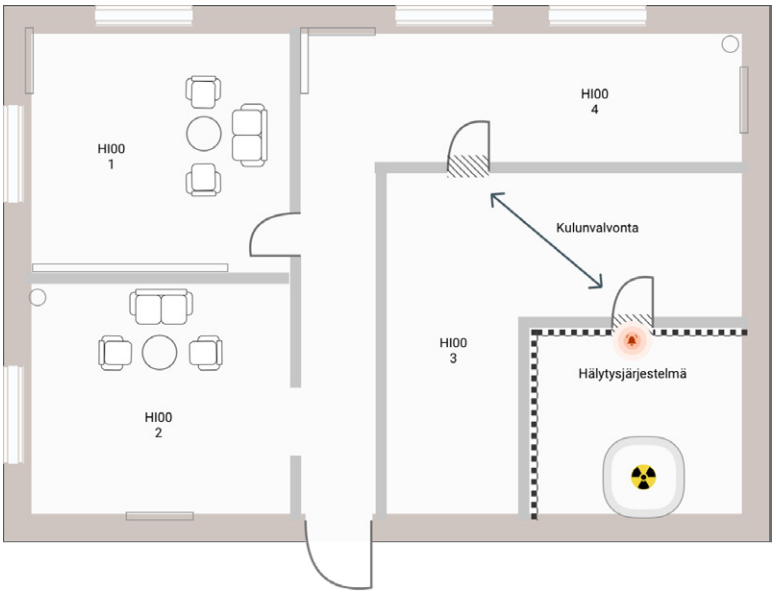
- Käyttötarkoitus voi tarkoittaa esimerkiksi sädehoitoa tai pinnankorkeuden mittaamista.

4 Kuvaus säteilylähteiden käyttö- ja säilytyspaikan sijainnista, turvajärjestelyjen tasosta, rakenteellisista esteistä, kulunvalvonnasta ja hälytysjärjestelmistä sekä kuva, johon on merkitty ainakin a) säteilylähteiden sijainti b) rakenteelliset esteet c) kulunvalvontajärjestelmät d) hälytysjärjestelmät

- Säteilylähteiden käyttö- ja säilytyspaikan sijainti, turvajärjestelyjen taso, rakenteelliset esteet, kulunvalvonta ja hälytysjärjestelmä on hyvä kuvailla mahdollisimman yksityiskohtaisesti.
- Voit selvittää myös mitä töitä käyttö- ja säilytyspaikalla tehdään ja kuinka monella sinne on kulkuoikeus.
- Selvitä turvajärjestelyjen taso ja miten tason vaatimukset täytetään.
- Selvitä tarkentavia tietoja rakenteellisista esteistä (mitä materiaalia rakenteet ovat), voit liittää myös kuvia.
- Selvitä tarkentavia tietoja pääsyoikeuksista, kulunvalvonnasta ja hälytysjärjestelmistä, esimerkiksi mihin hälytykset ohjataan.
- Kohdat a–d tulee merkitä pohjapiirrokseen tai kuvaan, joka liitetään suunnitelmaan.

5 Ohjeet tai viittaukset ohjeisiin, jotka koskevat a) säteilylähteiden säännöllisiä tarkistuksia b) toimintaa ja viestintää poikkeavissa tapahtumissa c) suunnitelman turvajärjestelyistä ja turvajärjestelyjen ajan tasalla pitämistä d) turvajärjestelyasiakirjojen käsittelyä ja säilyttämistä

- Selvitä myös ohjeiden sisältö lyhyesti.
- Selvitä miten ohjeiden ylläpito ja päivitys on suunniteltu.



KUVA 9. Esimerkki selkeästä kuvasta, johon on merkitty säteilylähteiden sijainti ja turvajärjestelmät. Suttuinen pohjapiirros, johon on tehty merkinnät käsin, on usein vaikeaselkoinen.

Turvajärjestelysuunnitelmaa päivittäessä tulisi tarkastella sen yhteensopivuutta pelastussuunnitelman kanssa ja vastaavasti pelastussuunnitelmaa päivittäessä yhteensopivuutta turvajärjestelysuunnitelman kanssa.

2.6 Tietoturvallisuus

7 § Toimet turvajärjestelyjen tasolla B

Suunnitelmia turvajärjestelyistä, menettelytapaohjeita ja muita vastaavia tietoja on käsiteltävä ja säilytettävä siten, että ne eivät päädy muiden henkilöiden haltuun kuin niiden, jotka tehtäviensä puolesta kyseisiä asiakirjoja tarvitsevat ja joille on myönnetty niihin pääsy.

Suojattavaa tietoa on esimerkiksi turvajärjestelysuunnitelma, lähdetiedot ja säteilylähteiden kuljetusta koskevat tiedot.

Teollisuusyritysten yleisimmät tietoon kohdistuvat rikokset ja väärinkäytökset 1) Tietoverkkoon murtautumisen tai hakkeroinnin yritykset 24 % (kaikkien vastaajien ka. 26 %) 2) Tietojen luvaton kopiointi ennen siirtymistä yrityksen palveluksesta 9 % (kaikkien vastaajien ka. 10 %) 3) Yritystiedon luvaton urkkiminen / yritysvakoilu 7 % (kaikkien vastaajien ka. 8 %). (Kauppakamari, Yritysten rikosturvallisuus 2017)

Keinoja tietoturvallisuuden toteuttamiseksi:

1 Yleistä
- Tiedot pidetään ajan tasalla ja tallessa.
- Tiedot ovat vain niiden käytössä, joilla on käyttötarve ja käyttöoikeus (luottamuksellisuus, käytettävyys, eheys).

2 Tietoaineistoturvallisuus suojattavalle tiedolle
- Ei-julkiset materiaalit tunnistetaan toiminnanharjoittajan toimesta.
- Käydään läpi ja tunnistetaan asiakirjat, joita voitaisiin käyttää lainvastaisessa toiminnassa hyväksi (kuten laitteen rakenteita ja toimintaa koskeva tieto).
- Tiedot luokitellaan ja merkitään tarvittaessa luottamukselliseksi.
- Tietoaineisto säilytetään lukitussa kaapissa, joka tarjoaa murtosuojaa ja palosuojaa.
- Tiedot tuhotaan luotettavasti (ylikirjoitus, silppuri).
- Sähköisessä välityksessä liikenne tai tieto suojataan tai salataan (suojattu verkko, julkisessa verkossa tieto salattuna).

3 Käyttöturvallisuus
- Työasemat lukitaan ja kirjaudutaan ulos laitteesta/järjestelmästä työn päätyttyä.
- Selvitetään, miten arkaluontoista tietoa säilytetään paperisena / sähköisenä käytännössä.
- Selvitetään, minkälaiset tietoturvajärjestelyt sähköiselle materiaalille on olemassa.

4 Tietojärjestelmäturvallisuus
- Käyttäjät tunnistetaan ja todennetaan luotettavasti.
- Riskienarvioinnin perusteella palomuurien ja haittaohjelmien torjunnan järjestelmät.
- Myös liikuteltavat laitteet, kuten matkapuhelimet ja kannettavat tietokoneet suojataan.

Tietoturvallisuuteen kuuluu myös turvallisuuskulttuuri: On painotettava, etteivät luottamukselliset asiat leviä suullisesti.

Yrityksistä 43 prosenttia tunnistaa, että niillä on tietotaitoa tai muuta omaisuutta, joka saattaisi olla laittoman tiedustelun kohteena. Edelleen merkittävä osa yrityksistä ei osaa sanoa, mitä tietoja ulkopuolinen tunkeutuja tai vaikkapa yrityksen oma työntekijä voisi viedä eli yrityksen liiketoiminnalle kriittistä tietoa ei tunnisteta. Yrityksen on hyvä myös tunnistaa yrityksen hallussa oleva asiakkaiden tai viranomaisten luottamuksellinen tieto.
(Kauppakamari, Yritysten rikosturvallisuus 2017)

Henkilökunnan koulutus on tärkeä keino edistää tietojen käsittelyohjeiden sisäistämistä ja ohjeiden noudattamista. Joka toisessa (54 %) yrityksessä henkilökuntaa koulutetaan salaisten tai luottamuksellisten tietojen käsittelyyn. Teollisuudessa ja rakennusalalla on vielä enemmän yrityksiä, joissa ei kouluteta salaisten tai luottamuksellisten tietojen käsittelyyn kuin yrityksiä, joissa koulutusta on. (Kauppakamari, Yritysten rikosturvallisuus 2017)

Erityisesti seuraava tieto tulee suojata:
- rakenteellista suojausta ja turvajärjestelyjä koskevat tiedot
- säteilylähteitä koskevat tiedot
- tietoteknisiä järjestelmiä koskevat tiedot, jotka liittyvät suorasti tai epäsuorasti turvallisuuteen
- jatkuvuus- ja ensivastesuunnitelmat
- tiedot liittyen turvajärjestelyistä vastaaviin henkilöihin, toimittajiin ja alihankkijoihin
- uhka-arviot.

2.7 Säteilylähteiden säännönmukainen tarkistus

7 § Toimet turvajärjestelyjen tasolla B

Toiminnanharjoittajan on tarkistettava vähintään kerran kuukaudessa, että sen vastuulla olevat turvajärjestelyjen tasoa B edellyttävät säteilylähteet ovat tallessa. Tarkistusten toteutus on dokumentoitava.

Säännönmukaista tarkistamista tehdään kerran kuukaudessa ja tarkistus dokumentoidaan. Tarkistus ja dokumentointi voidaan tehdä osana esimerkiksi huoltoa tai muuta tarkistusta, jossa säteilylähde todetaan tallessa olevaksi.

Säännönmukaisen tarkistuksen yhteydessä suositellaan seuraavaa:

- Tarkista, että säteilylähteen käyttöpaikalla ei säilytetä lähteitä, joita ei enää käytetä.
- Tarkista, että radioaktiivista ainetta, tai sellaista sisältävää laitetta ei varastoida tarpeettomasti. Tarpeellista varastointia voi olla esimerkiksi lyhytikäisen avolähteen aktiivisuuden pienentäminen varastoinnilla.
- Varmista turvallinen varastointi. Varastoitavien lähteiden käytölle laaditaan suunnitelma. Suunnitelmaa, lähteiden käyttöä ja säilytystarvetta arvioidaan vuosittain.

3 Turvajärjestelyjen taso A

Seuraavissa kappaleissa ohjeistetaan turvajärjestelyjen tason A vaatimusten toteuttamista siltä osin kuin ne poikkeavat kappaleessa 2 esitetyistä B-tason vaatimuksista.

3 § Turvajärjestelyjen taso A

Turvajärjestelyt on toteutettava tason A mukaisesti, jos:

1) **umpi- tai avolähteen aktiivisuus on suurempi tai yhtä suuri kuin STUKin määräyksen S/9/2021 liitteessä olevassa taulukossa esitetty aktiivisuus; tai**

2) **samassa käyttö- tai säilytyspaikassa olevilla umpi- ja avolähteillä toteutuu ehto**

$$\Sigma_n \frac{A_n}{R_n} \geq 1000 \text{ , missä}$$

A_n on radionuklidia n olevan yksittäisen umpi- tai avolähteen aktiivisuus ja samaa radionuklidia n sisältävien umpilähteiden yhteen laskettu aktiivisuus.

Avolähteen tapauksessa A_n on radionuklidia n sisältävän avolähteen suurin toiminnassa käytettävä aktiivisuus.

R_n on radionuklidin n liitteessä olevassa taulukossa esitetty aktiivisuus.

3.1 Rakenteelliset esteet

10 § Toimet turvajärjestelyjen tasolla A

Kaikkia rakenteellisia esteitä ei 8 §:ssä määrätystä poiketen voida korvata henkilöstön läsnäololla.

3.2 Suunnitelma turvajärjestelyistä

10 § Toimet turvajärjestelyjen tasolla A

Suunnitelma turvajärjestelyistä on tarkistettava säännöllisesti vähintään kolmen vuoden välein.

3.3 Kameravalvonta

10 § Toimet turvajärjestelyjen tasolla A

Säteilylähteiden käyttö- ja säilytyspaikka on varustettava etävalvontakameralla tai vastaavalla menettelyllä, jolla hälytyksen syy voidaan selvittää viivytyksettä.

Etävalvontakameraa tai vastaava menettelyä tulee käyttää silloin, kun säteilylähteen käyttö tai säilytyspaikalla ei ole läsnä henkilökuntaa. Huomioi suunnittelussa ajantasaiset säädökset kameravalvonnasta. Yleisiä tiloja ja työntekoa ei saa kuvata!

4 Turvallisuusjohtaminen

Säteilyn käytöstä vastuussa olevan organisaation johdon on huolehdittava siitä, että organisaation toiminnassa ylläpidetään ja kehitetään hyvää turvallisuuskulttuuria ja kaikilla tasoilla työskentelevät henkilöt, tehtäviensä mukaan

1. ovat tietoisia toimintaan ja suojelutoimiin liittyvistä säteilyriskeistä sekä ymmärtävät niiden turvallisuusmerkityksen
2. noudattavat turvallisia toimintatapoja
3. osallistuvat turvallisuuden jatkuvaan kehittämiseen.

Lisäksi organisaation johdon on huolehdittava, että turvallisuusjohtamisessa yhdistyvät menetelmien, toimintatapojen ja ihmisten johtaminen turvallisuuden hallitsemiseksi.

STUK antaa kansainvälisiin suosituksiin perustuen tarkemmat määräykset hyvän turvallisuuskulttuurin ylläpitämisestä ja edistämisestä sekä turvallisuusjohtamisesta.

Pohdi miten seuraavat kysymykset toteutuvat yrityksessänne:

- Ymmärretäänkö asioiden turvallisuusmerkitys kokonaisuuden ja pitkän aikavälin näkökulmasta oikein?
- Onko riskien tunnistaminen ja niiden käsittely huolellista?
- Kertooko työympäristö ja työolosuhteet pyrkimyksestä korkeaan laatutasoon ja huolellisuuteen?
- Kannetaanko vastuuta ja korjataanko puutteet ripeästi?
- Korostuuko turvallisuus johdon johtamistyylissä?

Toiminnanharjoittaja määrittää salassa pidettävään tietoon sekä turvallisuuteen liittyvät vastuut.

Organisaatio määrittää turvallisuuden hoitamisen tehtävät ja vastuut liittyen ainakin turvallisuuden hallintaan, henkilöstöturvallisuuteen, fyysiseen turvallisuuteen, tietoturvallisuuden hallintaan ja salassa pidettävän tiedon käyttöympäristön omistajan.

Turvallisuusdokumentaatiota ylläpidetään ja sen ajantasaisuutta seurataan säännöllisesti. Dokumentaatio kattaa salassa pidettävään tietoon liittyvät prosessit ja käsittelyn.

Riskienhallintaprosessia on syytä hyödyntää osana turvallisuusjohtamista. Lisätietoa: Kansallinen turvallisuusauditointikriteeristö KATAKRI.

5 Riskienhallinta

Tunnistamattomia riskejä vastaan on vaikea varautua.

KATAKRIn mukaan riskienhallinnassa tavoitellaan epäedullisten ja haitallisten tapahtumien välttämistä tai tapahtumien seurausten pienentämistä. Riskienhallinta on myös potentiaalisten vaarojen tunnistamista, analysointia ja hyödyntämistä.

Ohjeita riskienhallintaan:

- Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi.
- Riskien analysoinnissa on käytettävä vakiintunutta, avointa ja ymmärrettävää järjestelmällistä menetelmää.
- Riskienhallintaan osallistuvat kaikki tarvittavat tahot organisaation sisältä ja ulkopuolelta.
- Tunnistetut riskit on otettava huomioon tarvittavien sidosryhmien osalta.
- Riskienhallintaprosessia ja sen tuloksia hyödynnetään turvajärjestelyjen suunnittelussa ja soveltuvilta osin hankintoja suunnitellessa.
- Turvatoimien mitoituksessa huomioidaan muun muassa tiedon suojaustaso, määrä, muoto, luokitteluperuste ja sijoitustilat suhteessa arvioituun lainvastaisen toiminnan uhkaan.
- Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.

Riskienhallinnan tuloksena

- suojattavat kohteet on tunnistettu
- suojattaviin kohteisiin liittyvät riskit on tunnistettu ja arvioitu
- suojausmenetelmät on suhteutettu tunnistettuihin riskeihin
- organisaatiossa ylläpidetään kuvausta turvallisuusjärjestelyistä
- riskienhallintaprosessin johtopäätökset on huomioitu organisaation turvallisuusdokumentaatiossa.

Turvajärjestelyt voidaan toteuttaa yksittäisillä luotettavilla toimilla, tai useampia ratkaisuja yhdistämällä. Esimerkiksi rakenteellisen turvallisuuden vaikuttavuutta voidaan parantaa teknisillä turvajärjestelyillä, ja siten saavuttaa riskeihin nähden riittävä turvajärjestelyjen yhdistelmä. Lisätietoa: Kansallinen turvallisuusauditointikriteeristö KATAKRI.

Riskikartoituksen tekeminen on tehokas tapa selvittää, millaisia uhkia yritykseen kohdistuu. Tällöin yritys saa paljon tietoa siitä, mihin uhkiin sen kannattaa ensisijaisesti varautua ja mihin resurssit kannattaa kohdistaa. Kaikista vastaajayrityksestä 40 prosenttia oli tehnyt kirjallisen riskikartoituksen. (Kauppakamari, Yritysten rikosturvallisuus 2017)

6 Turvallisuuskulttuuri

Turvallisuuskulttuuri on kokonaisturvallisuuden käsite, johon sisältyvät sekä turvallisuus (safety), että turvajärjestelyt (security). Toiminnanharjoittajan tulee edistää turvallisuuskulttuuria, keinoja voivat olla esimerkiksi

- säännöt ja käytänteet, jotka tukevat käsitystä turvallisuuden tärkeydestä
- turvallisuuteen vaikuttavien ongelmien identifiointi ja korjaaminen viipymättä
- turvallisuuteen liittyvien vastuiden ilmoittaminen selvästi
- varmistaminen, että henkilökunta tuntee velvollisuutensa ja toimintansa turvallisuusmerkityksen
- varmistaminen, että henkilökunta on asianmukaisesti koulutettu
- varmistaminen, että henkilökunta on pätevää ja luotettavaa
- organisaation tekemät viestinnän järjestelyt, jotka edistävät turvallisuuteen liittyvän tiedon liikkumista: sekä onnistumisista, että epäonnistumisista viestitään
- salassa pidettävän informaation tunnistaminen ja suojaaminen
- toiminnanharjoittajan tekemä varmistus, että turvajärjestelyjä, määräyksiä ja hyvää turvallisuuskulttuuria toteutetaan käytännössä, eikä ainoastaan luetella toimia kirjallisesti.

Lisätietoa: World Institute for Nuclear Security WINS.

> Yrityksen johdon asenne turvallisuuteen ohjaa merkittävällä tavalla sitä, miten henkilökunta suhtautuu turvallisuuteen. Turvallisuuteen vähättelevästi suhtautuva henkilökunta voi tehdä tarkoittamattaan tyhjäksi sen, mitä yritys on tavoitellut panostaessaan turvallisuuteen. Jos henkilökunta päästää yritykseen tuntemattomia henkilöitä, voi sinänsä hyvää tarkoittava henkilökunta tehdä tyhjäksi sijoitukset ovien lukitukseen, hälytysjärjestelmiin ja vartiointiin. Henkilökunnan koulutus on tehokkain tapa kertoa henkilökunnalle, miten yritys haluaa henkilökunnan toimivan turvallisesti. (Kauppakamari, Yritysten rikosturvallisuus 2017)

Lisätietoa turvallisuuskulttuurista löytyy STUKin nettisivuilta.

7 Turvajärjestelyjä ja turvallisuutta täydentävät ratkaisut

Tässä luvussa esitellään esimerkkejä ja hyviä käytäntöjä turvallisuuden parantamiseksi säteilyn käyttöä harjoittavassa yrityksessä.

7.1 Rakenteellisten esteiden täydentäminen

Ankkurointi

Säteilylaitteen kiinnitys lattiarakenteeseen tai seinään voi toimia lisävarmistuksena estämään laitteen luvatonta siirtämistä. Ankkurointi on hyvä yhdistää hälytysjärjestelmään.

Turvakehikko

Yhdysvalloissa kehitetty ”In-device delay-kit” (IDD) on erityisesti verensäteilyttimiä ja terveydenhuollon säteilylaitteita varten suunniteltu ratkaisu, jossa laitteen ympärille rakennetaan eräänlainen turvakehikko. Kehikko on suunniteltu siten, että laitteen käytettävyys tai käytönaikainen turvallisuus eivät vaarannu. Kehikon ideana on hidastaa laitteen luvatonta siirtämistä tai säteilylähteen poistamista laitteesta. Jokainen IDD-kit tehdään tilauksesta ja asennetaan kyseiselle laitteelle sopivaksi.

Teknologiaan voi tutustua osoitteessa: www.energy.gov/nnsa/articles/meet-machine-enhancing-security-radiological-sources-through-device-delay-kits-idd.

7.2 Teknisten turvajärjestelmien täydentäminen

Liikuteltavien laitteiden paikannus

Erityisesti liikuteltavien radiografialaitteiden osalta GPS-paikannus voi toimia hyödyllisenä täydennyksenä muille turvajärjestelyille. Uusia laitteita hankkiessa on hyvä selvittää, onko laitteessa sisäänrakennettu GPS-paikannusmahdollisuus. Joihinkin laitetyyppeihin saattaa olla mahdollisuus liittää myöhemmin esimerkiksi RFID-merkintä. Paikannusmenetelmät eivät vähennä velvollisuutta huolehtia laitteesta, mutta mikäli laite joutuu hukkaan, se on mahdollista löytää helpommin.

7.3 Kiinteistö- ja toimitilaturvallisuus

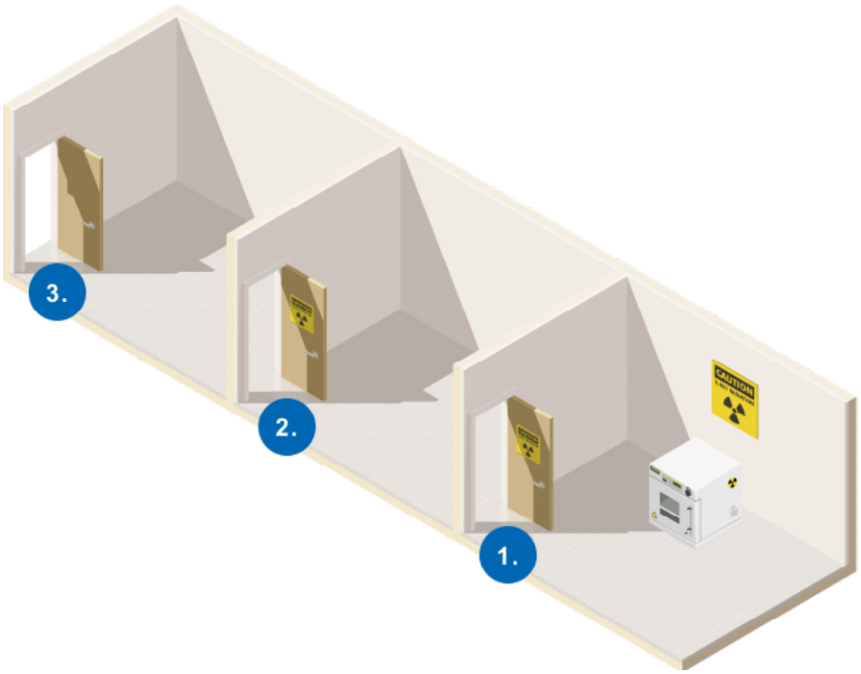
Riskiarvioinnin perusteella voidaan harkita tilojen luokittelua kiinteistö- ja toimitilaturvallisuuden periaatteiden mukaan. Yrityksen toimitilat luokitellaan eri turvallisuusvyöhykkeisiin ja muodostetaan kehäsuojaus rakenteellisten ja teknisten ratkaisujen avulla.

Aiheeseen voi perehtyä lisää esimerkiksi Elinkeinoelämän keskusliiton sivuilla ek.fi/hyotytietoa-yrityksille/yritysturvallisuus.

7.4 Varoitusmerkinnät

Säteilylähteistä varoittavia merkintöjä voi täydentää selvittävillä lisäteksteillä tai muilla vastaavilla menettelyillä. Erilaiset turvajärjestelyistä viestivät merkinnät lisäävät pelotevaikutusta, joka saattaa karkottaa lainvastaista toimintaa harkitsevan. Merkinnät voivat kuitenkin myös lisätä kiinnostusta lainvastaiseen toimintaan, jos niitä sijoitellaan harkitsemattomasti.

Merkin sisältämän varoituksen on oltava sellainen, että myös säteilysuojeluun perehtymätön henkilö ymmärtää sen. Jos säteilylähdettä käytetään tai säilytetään sille erityisesti varatussa tilassa, on käyttötilaan johtavassa ovessa tai sen välittömässä läheisyydessä oltava säteilyvaaraa osoittava merkki, kun on tarpeen varoittaa ionisoivan säteilyn aiheuttamasta vaarasta.



Kuva 10. Varoitusmerkkien sijoittelu.

Varoitusmerkin tarkoitus on kiinnittää huomio säteilyvaaraan. Kuvassa säteilylähteestä kauimmaista ovea ei ole merkitty. Merkit on sijoitettava siten, että ne eivät aiheettomasti herätä ulkopuolisten huomiota. Merkkien sijoittelu ei kuitenkaan saa johtaa säteilyturvallisuuden heikentymiseen. Tässä tapauksessa kaksi ensimmäistä merkintää parantavat säteilyturvallisuutta, kolmas ovi on jo sellaisella vyöhykkeellä, johon voisi olla laajemmat kulkuoikeudet ja merkintä saattaisi aiheuttaa tarpeetonta kiinnostusta.)

Myös pelastustoimintaa voi edesauttaa helpoilla ratkaisuilla. Säteilylähteet tai säteilyvaara on hyvä merkitä pohjapiirrokseen, joka säilytetään paloilmoitinkaapissa. Mikäli paloilmoitinkaappeja on useampi, on ne syytä merkitä jokaiseen.

Toiminnanharjoittaja voi harkita, olisiko lattiaan mahdollista merkitä säteilyvaaramerkinnät pelastustoiminnan turvallisuuden kehittämiseksi. Merkinnät seinissä ja ovissa peittyvät savuun tulipalon sattuessa, mutta lattiassa olevat merkinnät saattavat näkyä.

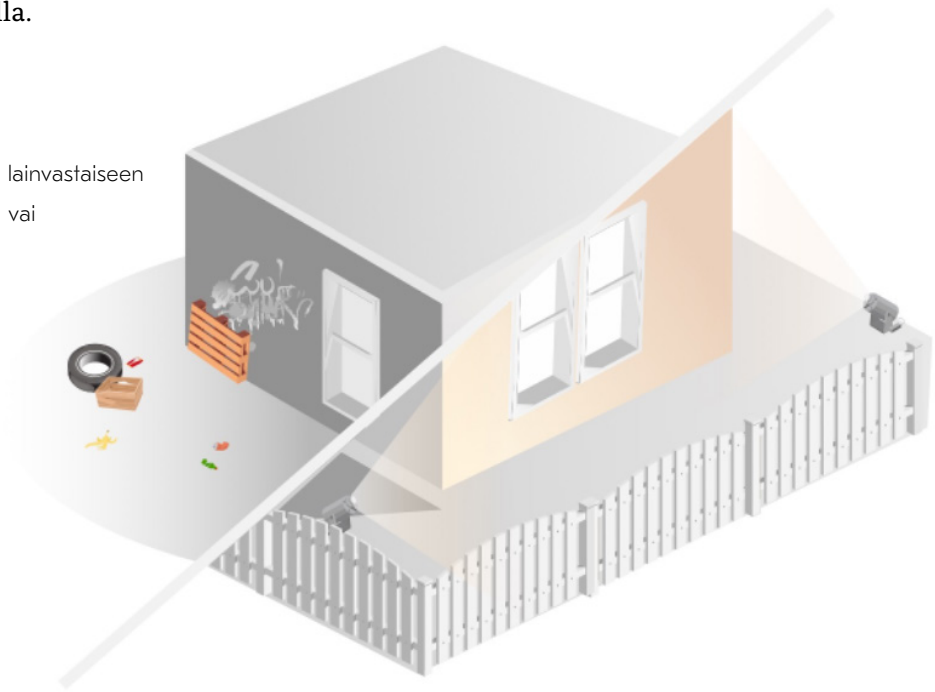
Toiminnanharjoittajan kannattaa sopia käytänteistä yhdessä paikallisen pelastuslaitoksen ja poliisin kanssa. Viranomaisille kannattaa tarjota mahdollisuutta vierailla toimipaikalla tutustumassa siihen, miten säteilylähteet vaikuttavat esimerkiksi pelastustoiminnan turvallisuuteen. Viranomaiset voivat myös testata omien säteilymittareidensa käyttöä ja toimintaa.

7.5 Rikostentorjunta ympäristösuunnittelun avulla

CPTED-malli tarkoittaa vapaasti käännettynä rikostentorjuntaa ympäristösuunnittelun avulla. Suunnittelun tuloksena voidaan esimerkiksi lisätä ulkoalueiden valaistusta pimeällä tai raivata kasvustoa, jonka suojaan lainvastaista toimintaa suorittava voisi piiloutua, suojattavan rakennuksen ympäriltä. Tarkoituksena on luoda selkeä ympäristö, josta poikkeava käyttäytyminen on helppo havaita ja poistaa tiloja, johon ei haluta ulkopuolisia.

Rikostentorjunta ympäristösuunnittelun avulla pyrkii estämään lainvastaisen toiminnan tapahtumista luomalla puitteet, jotka vähentävät rikoksen houkuttelevuutta tai poistamaan kokonaan tilaisuuden rikoksen tekemiselle. Mikäli suunnittelu on onnistunut, sen tuloksena rikoksen tekeminen vaikeutuu, mikä puolestaan vähentää lainvastaisen toiminnan todennäköisyyttä.

Luontaisia elementtejä voi täydentää esimerkiksi jatkuvalla tai liiketunnistimesta käynnistyvällä valaistuksella.



KUVA 11. Kumpi kutsuu enemmän lainvastaiseen toimintaan, hämyinen ja sotkuinen vai aidattu ja valaistu seinusta?

CPTED –ajatteluun pohjautuvaan suomenkieliseen materiaaliin rakennetun ympäristön turvallisuudesta voi tutustua osoitteessa rikoksentorjunta.fi/rakennetun-ympariston-turvallisuus.

7.6 Tunkeutumisreittianalyysi

Toiminnanharjoittaja voi perehtyä toimitilaturvallisuuteen liittyvien rakenteellisten ratkaisujen riittävyyteen tunkeutumisreittianalyysin avulla. TUREAN-tunkeutumisreittianalyysin avulla tunnistetaan tilojen suojaukseen liittyvien ratkaisujen tehokkuus.

Tunkeutumisreittianalyysi löytyy ohjeineen osoitteesta www.yhteisturvallisuus.net/materiaali.html.

Tunkeutumisreittianalyysiä on tutkittu ja kehitetty eteenpäin opinnäytetyönä, joka löytyy vapaasti luettavasta Theseus-palvelusta.

7.7 Turvallisuusviestintä

Yrityksen sisäisen viestinnän tavoitteena voi olla yhteistyön tehostaminen, tietoisuuden lisääminen sekä oikean tiedon välittäminen. Turvallisuusasioista tulisi viestiä samoin tavoittein. Poikkeamia tai turvallisuusongelmia ei tule piilottaa ja salata vaan tiedottaa ja korjata.

Turvallisuusasioista ja luottamuksellisista asioista on hyvä tehdä ohjeet henkilökunnalle, jotta viestintä olisi tehokasta, mutta tietoturvallista.

> Kaikissa yrityksissä on luottamuksellisen tiedon lisäksi yrityksen sisäistä tietoa ja julkista tietoa. Liike- ja ammattisalaisuuksien käsittelyä koskevan ohjeen lisäksi työnantajan kannattaisi tehdä myös muita tietoja koskeva käsittelyohje tai sisällyttää nämä samaan ohjeeseen. Yksinkertaisimmillaan ohje voi jakaa kaikki yrityksen tiedot julkisiin ja sisäisiin tietoihin. Ohjeet voidaan sisällyttää yrityksen omiin yleisiin ohjeisiin tai sitten niistä voidaan laatia omat erilliset ohjeet vain niille, jotka käsittelevät tietoa. (Kauppakamari, Yritysten rikosturvallisuus 2017)

7.8 Säteilyturvallisuuspoikkeamiin varautuminen

Säteilyturvallisuuspoikkeama voi olla säteilyn käytön normaalitilanteesta poikkeavan tilanteen lisäksi myös säteilylähteiden katoaminen tai varastetuksi joutuminen. Poikkeavia tapahtuma varten on syytä varautua.

Varautuminen voidaan aloittaa esimerkiksi tekemällä riskien arviointia, jonka perusteella turvajärjestelyjä suunnitellaan, toteutetaan ja päivitetään. Poikkeavassa tilanteessa toimimisen harjoittelu on tärkeä osa varautumista. Lisätietoa turvallisuuskulttuurista löytyy STUKin nettisivuilta. nettisivuilta.

Kun yritys tekee toimintaohjeen poikkeustilanteita varten, varautuu yritys samalla myös jatkuvuuttaan tavalla tai toisella uhkaaviin tilanteisiin. Jatkuvuutta uhkaavan tilanteen käynnistyessä ensimmäinen toimenpide on käynnistää poikkeustilanteen toimintaohjeiden mukainen toiminta keräämällä poikkeustilanteiden johtoryhmä koolle. Suurista vastaajayrityksistä yhdeksän kymmenestä on laatinut poikkeustilanteen toimintaohjeen ja keskisuurista kaksi kolmasosaa.
(Kauppakamari, Yritysten rikosturvallisuus 2017)

7.9 Huoltojärjestelyt

Toiminnanharjoittajan toimittamassa turvallisuuslupahakemuksessa selvitetään säteilylähteitä sisältävien laitteiden huoltojärjestelyt.

Toiminnanharjoittaja varmistaa, että säteilyturvallisuusvastaava sekä huoltotyötä tekevät henkilöt

- ovat saaneet työn vaatiman koulutuksen
- hallitsevat laitteiden käyttöön ja huoltotyön turvallisuuteen liittyvät asiat
- tekevät työn turvallisesti.

Huoltotöissä on huomioitava, etteivät turvajärjestelyt vaarannu. Huoltotöitä suoritettaessa lähteen käyttö- tai säilytyspaikalla vaatimukset esimerkiksi rakenteellisten esteiden määrästä tulee täyttyä. Mikäli säteilylähde siirretään huoltoon valmistajalle, on myös kuljetuksessa huomioitava turvajärjestelyt ja radioaktiivisten aineiden kuljetuksessa vaarallisten aineiden kuljetusmääräykset.

Turvajärjestelmiä tulee ylläpitää valmistajan ohjeiden mukaan.

Toiminnanharjoittajan tulee arvioida oman turvajärjestelmänsä toimivuutta ja seurata turvajärjestelyjen hyviä käytäntöjä ja teknologian kehitystä.

7.10 Itsearviointi ja auditoinnit

Yrityksen sisäinen tarkastus, turvallisuuskävely, havainnointi ja auditointi voivat olla keinoja

- riskienhallinnan tueksi
- turvajärjestelyjen toimivuuden ja toteutumisen arviointiin
- turvajärjestelyjen tehostamisen pohjatiedoksi.

Tarkastelu voi koskea esimerkiksi turvallisuuskulttuuria tai tiettyä turvajärjestelyä.

Toiminnanharjoittajan omien tarkistusten avulla voidaan löytää puutteita ja kustannustehokkaita mahdollisuuksia turvajärjestelyjen kehittämiselle sekä valmistautua STUKin tarkastukselle. Myös ulkoisella auditoinnilla voidaan arvioida yrityksen yleistä turvallisuuden tasoa tai turvajärjestelyjä.

Turvallisuuskävelyt on hyvä toteuttaa yrityksen turvallisuuskoulutuksen yhteydessä. Turvallisuuskävelyssä kierretään oma, tuttu työpaikka ja tehdään havaintoja työpaikan riskeistä ja vaaranpaikoista. Työntekijät oppivat ehkäisemään vaaratilanteita, tutustuvat alkusammutuskalustoon ja muuhun turvallisuustekniikkaan. (SPEK)

7.11 Perehdytys ja koulutus

Pelkkien ohjeiden laatimisen sijaan turvallisuuteen liittyvää koulutusta on suositeltavaa järjestää.

Sisältönä voi olla esimerkiksi

- toiminta poikkeavan tapahtuman sattuessa
- yrityksen turvajärjestelyt
- kulunvalvonnan periaatteet
- henkilökunnan kulkuoikeudet
- avainten ja tunnusten käyttö ja säilyttäminen
- henkilökunnan liikkuminen
- henkilökortin käyttö
- hälytykset vartiointiliikkeelle
- yrityksen tiloissa vierailevat ulkopuoliset henkilöt
- turvallisuuden edistäminen omilla toimilla
- toimintaohjeet, jos rikos tai vahingonteko havaitaan tai sellaista epäillään
- asiakirjaturvallisuus
- säteilyturvallisuus
- työturvallisuus jne.

Käsittelemällä turvallisuusasioita henkilökunnan kanssa saadaan työntekijät aktivoitua turvallisuusasioihin ja ymmärtämään roolinsa osana yrityksen turvallisuutta. Turvallisuusasioiden käsittely osana liiketoiminnan kokouksia, kuten kuukausipalavereissa ja projektikokouksissa, tuo turvallisuuden osaksi liiketoimintaa ja lisää turvallisuustietoisuutta. (Kauppakamari, Yritysten rikosturvallisuus 2017)

7.12 Sisäinen uhka

Sisäinen uhka eli ns. **insider threat** tarkoittaa lainvastaisen toiminnan uhkaa yrityksen työntekijän tai toimipaikalla väliaikaisesti työskentelevän suorittamana. Esimerkiksi valvonnalla ja hyvällä turvallisuuskulttuurilla voidaan pienentää sisäisen uhkan riskiä. Ennaltaehkäisevänä toimena toiminnanharjoittaja voi harkita turvallisuusselvityksen tekemistä.

Turvallisuusselvityslain (726/2014) 21 momentin viidennen kohdan mukaan suppean turvallisuusselvityksen tekeminen henkilöille, joilla on pääsy työtehtäviensä vuoksi korkea-aktiivisten lähteiden luo, on mahdollista. Toiminnanharjoittajan tulee harkita, onko turvaselvityksen tekeminen järkevää.

Kulunvalvonnan laadukas toteutus, siihen liittyvät yrityksen ohjeet ja menettelytavat voivat pienentää huomattavasti ”**insiderin**” mahdollisuuksia päästä käsiksi säteilylähteisiin.

Liite 1
Lisätietoa ja ohjeita

Avainturvallisuus
www.finanssiala.fi/julkaisut/avainturvallisuusohje-2

IAEA NSS 11 – Security of Radioactive Sources
www-pub.iaea.org/MTCD/publications/PDF/Pub1387_web.pdf

Kamerat päivittäisenä turvanasi
www.finanssiala.fi/julkaisut/kameravalvontaesite-2

Kameravalvontaopas
www.finanssiala.fi/julkaisut/kameravalvontaopas-2

Kassakaappiohje
www.finanssiala.fi/julkaisut/kassakaappiohje-2

KATAKRI (Versio II, 2011)
www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

KATAKRI (Versio III, 2015)
www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_
auditointityokalu_viranomaisille.pdf

KATAKRI (Versio IV, 2020)
um.fi/documents/35732/0/Katakri+-+2020_1218.pdf

Kotien murtosuojaohje
www.finanssiala.fi/julkaisut/kotien-murtosuojausohje-2

Rakenteellinen murtosuojausohje I
www.finanssiala.fi/julkaisut/rakenteellinen-murtosuojaus-i-2

Rakenteellinen murtosuojausohje II
www.finanssiala.fi/julkaisut/rakenteellinen-murtosuojaus-ii-2

Rakenteellinen murtosuojausohje III
www.finanssiala.fi/julkaisut/rakenteellinen-murtosuojaus-iii-2

Suomen Riskienhallintayhdistys.
Materiaalia ja työvälineitä riskienhallinnan toteuttamiseen
pk-rh.fi

Ulkona säilytettävä omaisuus
www.finanssiala.fi/julkaisut/ulkona-sailytettava-omaisuus-2

Yhteisturvallisuus.net. Materiaalia turvallisuusjohtamiseen ja Tunkeutumisreittianalyysiin liittyen.
www.yhteisturvallisuus.net/materiaali.html

ISBN 978-952-309-561-8 (pdf)
ISSN 1799-9472

STUK
Säteilyturvakeskus
Strålsäkerhetscentralen
Radiation and Nuclear Safety Authority

Jokiniemenkuja 1
01370 Vantaa
Puh. (09) 759 881 (vaihde)
www.stuk.fi