Vesihuollon fyysisen turvallisuuden opas

Vesilaitosyhdistyksen monistesarja nro 106

Helsinki, 2026

Julkaisun jakelu:

Vesilaitosyhdistys
Ratamestarinkatu 7 B
00520 Helsinki

puh. (09) 868 9010
sähköposti: vvy@vvy.fi
kotisivu www.vvy.fi

ISSN-L 2242-7279
ISSN 2954-2014 (verkkojulkaisu)

ISBN 978-952-7545-35-5

Helsinki 2026

KUVAILULEHTI	
Julkaisija	Suomen Vesilaitosyhdistys ry
Tekijät	Seclion Oy Emilia Jaatinen, Hanna Erkinjuntti, Juha Laamanen
Julkaisun nimi	Vesihuollon fyysisen turvallisuuden opas
Julkaisusarjan nimi ja numero	Vesilaitosyhdistyksen monistesarja nro 106
Julkaisun teema	Fyysinen turvallisuus
Saatavuus	Julkaisu on saatavissa Vesilaitosyhdistyksen verkkosivuilta.
Tiivistelmä	Vesihuolto on yksi yhteiskunnan tärkeimmistä peruspalveluista, sillä se turvaa puhtaan veden saatavuuden ja jäteveden turvallisen käsittelyn kaikissa olosuhteissa. Vesihuollon luotettavuus on välttämätön niin arjen sujuvuudelle kuin yhteiskunnan kriittiselle toiminnalle. Lisäksi vesihuolto on keskeinen osa varautumista ja häiriötilanteiden hallintaa, jotta palvelut voidaan turvata myös poikkeusoloissa. Vesihuollon toimintaympäristö on muuttunut mm. geopoliittisen toimintaympäristön kehittymisen myötä sekä yleisen turvallisuustilanteen muutoksen seurauksena. Näiden muutosten seurauksena vesihuoltolaitokset ovat aiempaa todennäköisempiä kohteita erilaisille fyysisille turvallisuusuhille. Vesihuollon fyysisten rakennusten ja muiden kohteiden turvallisuuden kehittäminen on avainasemassa kokonaisturvallisuuden ja toiminnan jatkuvuuden varmistamisessa. Vesihuollon kohteiden fyysiseen turvallisuuteen ei ole aiemmin ollut käytettävissä alan yhteisiä ohjeita tai minimisuosituksia eikä myöskään selkeitä viranomaismääräyksiä. Oppaan sisältö käsittelee fyysisen suojauksen keinovalikoimaa, jonka lisäksi halutun suojausvaikutuksen saamiseksi oppaassa käsitellään myös käyttäjiin ja suojauskeinojen hallinnointiin liittyviä asioita. Organisaation fyysinen turvallisuus syntyy rakenteellisen turvallisuuden, teknisten turvajärjestelmien ja niiden käyttäjien sekä palveluntarjoajien toiminnan yhteisvaikutuksena.
Avainsanat	Fyysinen turvallisuus, rakenteellinen suojaus, turvatekniset järjestelmät, kulunhallinta, pääsynhallinta, kehäsuojausmalli
Rahoittaja/ toimeksiantaja	Suomen Vesilaitosyhdistys ry
	ISBN 978-952-7545-35-5 / *ISSN* 2954-2014
	Sivuja 88 / *Kieli* suomi / *luottamuksellisuus* julkinen
Julkaisun jakelu	Vesilaitosyhdistys, www.vvy.fi
	Tekijät vastaavat julkaisun sisällöstä eikä julkaisun sisältöä voida tulkita Vesilaitosyhdistyksen kannanotoksi.

DESCRIPTION			
Publisher	Finnish Water Utilities Association (FIWA)		
Authors	Seclion Oy Emilia Jaatinen, Hanna Erkinjuntti, Juha Laamanen		
Publication titel	Water Services Physical Security Guide		
Publicationserie's titel and number	Publication series of Finnish Water Utilities Association no. 106		
Publication theme	Physical Security		
Availability	Publication is available on the FIWA website		
Abstract	Water services are one of the most essential public utilities, ensuring the availability of clean water and the safe treatment of wastewater under all conditions. The reliability of water services is critical not only for the smooth functioning of everyday life but also for the continuity of society's vital operations. In addition, water services play a central role in preparedness and the management of disruption situations, ensuring that services can be maintained even under exceptional circumstances. The operating environment of water services has evolved due to, among other factors, geopolitical developments and changes in the overall security situation. As a result of these changes, water utilities have become more likely targets of various physical security threats. Strengthening the security of physical facilities and other water service assets is therefore key to ensuring overall security and operational continuity. Until now, there have been no common sector-wide guidelines, minimum recommendations, or clear regulatory requirements for the physical security of water service facilities. The guide addresses the range of physical protection measures and, in order to achieve the desired level of protection, also considers aspects related to users and the management of security measures. An organization's physical security is formed through the combined effect of structural solutions, technical security systems, and the actions of their users and service providers.		
Keywords	Physical security, structural protection, technical security systems, access control management, perimeter protection model		
Financer/ordering party	Finnish Water Utilities Development Fund, Finnish Water Utilities Association (FIWA)		
	ISBN 978-952-7545-35-5	*ISSN* 2954-2014	
	Pages 88	*Language* Finnish	*Confidentiality* Public
Distribution of the publication	Finnish Water Utilities Association (FIWA), www.vvy.fi		

Sisällysluettelo

1 Johdanto ... 1
1.1 Hankkeen tausta ja tarkoitus ... 1
1.2 Lainsäädännöllinen ja normatiivinen tausta ... 2
1.3 Hankkeen rajaukset ... 3
1.4 Hankkeen kohderyhmät ... 4
1.5 Termit ja määritelmät ... 4
1.6 Oppaan käyttö ... 8
2 Hallinnollisen turvallisuuden toteuttaminen ... 10
2.1 Turvallisuusjohtamisen ja turvallisuuden kehittämistyön perusteet ... 10
2.2 Hallinnollisen turvallisuuden merkitys ... 14
2.3 Turvallisuuspolitiikan merkitys ... 15
2.3.1 Tilojen oikeanlainen käyttö ... 17
2.3.2 Tietojen ja järjestelmien oikeanlainen käyttö ... 18
2.3.3 Avainhallinta ... 19
2.3.4 Yhteiskäyttölukot ja kolmannet osapuolet ... 21
2.3.5 Henkilöresurssien hallinta ... 22
2.3.6 Dokumentaation hallinta ... 26
2.4 Turvallisuustoimien kehittämisestä saavutettava hyöty ... 27
3 Riskienarviointi ja riskienhallinta ... 29
3.1 Riskien arvioiminen ... 29
3.2 ISO 31000 -viitekehys ja periaatteet ... 29
3.3 Riskienhallintaprosessin rakenne ... 30
3.3.1 Toimintaympäristön määrittäminen ... 31
3.3.2 Riskien arviointiprosessi ... 32
3.3.3 Riskien käsittely ... 32
3.3.4 Käytännön arviointiprosessi vesihuollossa ... 33
4 Fyysinen turvallisuus ... 35
4.1 Fyysisen turvallisuuden perusteet ... 35
4.2 Fyysisen turvallisuuden kokonaisuus ja riippuvuussuhteet ... 38
4.3 Kriittisyyden arviointi ... 39
4.4 Kehäsuojausmalli ja vyöhykkeet ... 41
4.5 Rakenteellinen suojaus ... 42
4.5.1 Aidat ... 42
4.5.2 Henkilöportit ... 43
4.5.3 Ajoneuvoportit ... 44
4.5.4 Seinät, katot ja lattiat – rajaavat rakenteet ... 45
4.5.5 Ajoneuvohidasteet ja -esteet ... 45
4.5.6 Ovirakenteet ... 46
4.5.7 Ikkunat, aukot ja luukut ... 46
4.5.8 Valaistus ... 47
4.5.9 Kyltit sekä kielto- ja varoitusmerkit ... 47
4.6 Turvatekniikan järjestelmät ... 48
4.6.1 Kameravalvontajärjestelmät ... 48
4.6.2 Kulunvalvontajärjestelmät ... 50
4.6.3 Murtohälytysjärjestelmät ... 52
4.6.4 Elektromekaaniset lukitusjärjestelmät ... 53
4.6.5 Mekaaniset lukitusjärjestelmät ... 53
4.6.6 IoT-sensorit ... 55
4.6.7 Tiedonkeruualustat tiedon koontiin ja tilannekuvan ylläpitoon ... 55
4.7 Palvelut ja toimintamallit ... 56
4.8 CPTED-malli – Rikosten ehkäisy ympäristön suunnittelun keinoin ... 57

4.9 Jatkuvuuden varmistaminen normaalioloissa 59
4.10 Fyysiset tunkeutumistestaukset 62
5 Fyysisen turvallisuuden elinkaari 64
5.1 Esisuunnitteluvaihe – uudis- tai saneerauskohde 64
5.1.1 Uudisrakennushankkeen esisuunnitteluvaihe 64
5.1.2 Saneeraushankkeen esisuunnitteluvaihe 64
5.2 Perussuunnitteluvaihe 65
5.2.1 Vastuut ja rajapinnat sekä resurssit ja osaaminen 66
5.2.2 Teknologian kehityksen huomioiminen 66
5.2.3 Resurssien kohdentaminen ja minimitason varmistaminen 66
5.3 Hankintavaihe ja tietoturva hankinnassa 67
5.3.1 Hankintavaiheen vähimmäisvaatimuksia 67
5.3.2 Tietoturvallisuus hankinnan aikana 69
5.4 Toteutus- ja urakointivaihe 70
5.5 Käyttöönotto ja käytön aikainen toiminta 71
5.5.1 Käytön aikainen hallinta 72
5.5.2 Takuuaika ja huoltovelvoitteet 72
5.6 PTS-suunnittelu ja omaisuudenhallintasuunnitelma 73
5.6.1 Turvatekniikan elinkaari 73
5.6.2 Esimerkki fyysisen turvallisuuden vuosikellosta 75
6 Poikkeusoloihin varautuminen 76
6.1 Miten varaudutaan? 76
6.2 Valmius korjata materiaalisia tuhoja 78
6.3 Resurssit poikkeusoloissa 78
6.3.1 Henkilövaraukset 78
6.3.2 Autojen ja työkoneiden varaaminen 79
7 Lähteet 80
8 Kuva- ja taulukkoluettelo 81
Liitteet 82

LIITE 1 OHJAAVAT MUUT ASIAKIRJAT
LIITE 2 FYYSISEN TURVALLISUUDEN HINTA-ARVIOT
LIITE 3 KEHÄSUOJAUSMALLIN ESIMERKKIRATKAISUT
LIITE 4 KULUNHALLINNAN JA PÄÄSYNHALLINNAN PERIAATTEET
LIITE 5 VESIHUOLTOLAITOKSEN NYKYTILAN ESIARVIOINTI
LIITE 6 TYÖKALU FYYSISEN TURVALLISUUDEN ARVIOINTIIN

Liitteiden tietoluokka:
TLP Amber - Rajattu organisaatioiden sisäinen käsittely

1 JOHDANTO

1.1 HANKKEEN TAUSTA JA TARKOITUS

Vesi on elämän perusedellytys ja korvaamaton resurssi kaikille. Suomessa meillä on harvinainen etuoikeus: puhdas ja laadukas vesi on maailmanlaajuisestikin ainutlaatuinen luonnonvara, jota on suojeltava vastuullisesti myös tuleville sukupolville. Vesihuoltolaitosten ydintehtävä on varmistaa vedenkäsittelyprosessin toimivuus ja veden laatu – tämä on se perusta, johon kaikki muu rakentuu.

Vesihuolto on yksi yhteiskunnan tärkeimmistä peruspalveluista, sillä se turvaa puhtaan veden saatavuuden ja jäteveden turvallisen käsittelyn kaikissa olosuhteissa. Suomessa vesihuolto perustuu korkeaan laatuun ja toimintavarmuuteen: raakavesi otetaan pääosin pohjavedestä ja käsitellään huolellisesti ennen jakelua, ja laaja verkosto varmistaa veden toimituksen kuluttajille. Käytetty vesi johdetaan viemäriverkoston kautta puhdistamoihin, joissa se käsitellään ympäristöä suojellen. Vesihuollon luotettavuus on välttämätön niin arjen sujuvuudelle kuin yhteiskunnan kriittiselle toiminnalle, ja sen ylläpitoon panostetaan jatkuvasti. Lisäksi vesihuolto on keskeinen osa varautumista ja häiriötilanteiden hallintaa, jotta palvelut voidaan turvata myös poikkeusoloissa.

Vesihuollon toimintaympäristö on muuttunut mm. geopoliittisen toimintaympäristön kehittymisen myötä sekä yleisen turvallisuustilanteen muutoksen seurauksena. Näiden muutosten seurauksena vesihuoltolaitokset ovat aiempaa todennäköisempiä kohteita erilaisille fyysisille turvallisuusuhille. Vesihuollon fyysisten rakennusten ja muiden kohteiden turvallisuuden kehittäminen on avainasemassa kokonaisturvallisuuden ja toiminnan jatkuvuuden varmistamisessa. Lisäksi vesihuollon kohteiden fyysisen turvallisuuteen ei ole ollut käytettävissä alan yhteisiä ohjeita tai minimisuosituksia eikä myöskään selkeitä viranomaismääräyksiä. Turvallisuus ei ole itsetarkoitus, vaan tukitoiminto, joka mahdollistaa ydintehtävän sujuvan ja häiriöttömän toteutumisen. VESFY-hankkeessa on pureuduttu siihen, mitkä fyysisen turvallisuuden elementit ovat erityisen merkityksellisiä vesihuoltoalalla ja minkälaisin keinoin niitä tulee suojata huomioiden vesihuollon kriittinen luonne.

Paraskaan lukko ei voi täyttää tehtäväänsä, jos sitä ei käytetä oikein. VESFY-hankkeen fokus on fyysisen suojauksen keinoissa, mutta halutun suojausvaikutuksen saamiseksi on välttämätöntä käsitellä myös käyttäjiin ja suojauskeinojen hallinnointiin liittyviä asioita. Organisaation fyysinen turvallisuus syntyy rakenteellisen turvallisuuden, teknisten turvajärjestelmien ja niiden käyttäjien sekä palveluntarjoajien toiminnan yhteisvaikutuksena.

VESFY-hankkeen lopputuotokset ovat:

- Vesihuollon fyysisen turvallisuuden opas ja sen liitteet
- Oppaaseen liittyvä erillinen työkalu fyysisen turvallisuuden suojauskeinojen suosituksista.

Opas antaa perustietoa fyysisen turvallisuuden perusperiaatteista sekä erilaisista toteutustavoista eri kokoisissa laitoksissa. Työkalun avulla yksittäisen vesihuoltolaitoksen on mahdollista arvioida oman laitoksensa kriittisyysluokka, tunnistaa oman toimintansa

kannalta kriittisimmät tilat, toiminnot ja prosessit sekä niiden suojauksen nykytila ja verrata nykytilaa annettuihin suosituksiin. Oppaan käytöstä kerrotaan tarkemmin **luvussa 1.6**.

Oppaan tavoitteet:

- Auttaa alan toimijoita ymmärtämään, miten turvallisuuden eri elementit liittyvät heidän omaan ydintehtäväänsä ja miten ne voivat tukea ja vahvistaa päivittäisen toiminnan kestävyyttä.
- Tarjota periaatteita ja ohjenuoria turvallisuushankkeiden suunnittelua ja läpivientiä varten
- Luoda yhtenevät käytännöt alalle ja antaa myös pienille laitoksille eväitä turvallisuustoimintaan.
- Asettaa standardi vesihuoltoalan fyysisen suojauksen toteutuskeinoille.

Opas ei sisällä erillistä työkalua yhdenmukaisen kypsyystason mittaamiseen, vaan pyrkii antamaan suosituksia ja välineitä oppaan tietojen ja sitä tukevien liitemateriaalien avulla. Käytännön näkökulmasta oppaassa korostuu taloudellinen tasapaino: miten valita ratkaisuja, jotka tarjoavat parhaan hyödyn ja vaikutuksen eri hintahaarukoissa. Turvallisuusinvestointien ei tulisi rasittaa taloutta, vaan ne tulee suunnitella osaksi kokonaisvaltaista ja pitkäjänteistä vesihuollon kehittämistä.

Yhteiskunnallisessa mittakaavassa vesihuoltolaitosten tekemät panostukset fyysiseen turvallisuuteen osoittavat, että turvallisuus on laitosten toiminnan keskiössä, mikä edelleen lisää kansalaisten luottamusta yhteiskunnan toiminnan varmuuteen.

Hanketta on rahoittanut Vesilaitosyhdistyksen kehittämisrahasto sekä hankkeeseen myös osallistuneet 11 vesilaitosta, jotka ovat Alva-yhtiöt Oy, Hämeenlinnan Seudun Vesi Oy (HS-Vesi), Kuopion Vesi Oy, Lahti Aqua Oy, Oulun Vesiliikelaitos, Porin Vesi, liikelaitos, Tampereen Vesi Oy, Turun Vesihuolto Oy, Kymen Vesi Oy ja Kouvolan Vesi Oy. Lisäksi osallistuneet vesilaitokset tuottivat kukin hankkeelle ohjausryhmätyön, työpajatyön ja kommentointien kautta yhden tai kahden henkilön työpanoksen, joka on vesilaitosten osalta mittava panostus hankkeen sisällön ja laadun suhteen.

1.2 LAINSÄÄDÄNNÖLLINEN JA NORMATIIVINEN TAUSTA

Opas auttaa vesihuoltoalan toimijoita vastaamaan Euroopan unionin CER- ja NIS2-direktiivien vaatimuksiin.

- **CER-direktiivi** (The Critical Entities' Resilience directive) on tullut voimaan vuonna 2023 EU-tasolla. Suomessa se pannaan täytäntöön uudella lailla yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriöntietokyvyn parantamisesta (310/2025). Laki on tullut voimaan 1.7.2025. CER-direktiivin tavoite on kriittisten organisaatioiden häiriönsietokyvyn varmistaminen huomioiden kaikki luonnon ja ihmisen aiheuttamat riskit. CER koskee vesihuollon toimialaa sisältäen sekä talousveden tuotannon että jäteveden käsittelyn.
- **NIS2-direktiivi** (Directive on security of Networks and Information Systems) on tullut voimaan huhtikuussa 2025 ja pannaan täytäntöön kyberturvallisuuslain kautta. NIS2 koskee vesihuollon toimialan osalta sekä talousveden tuotantoa että jäteveden käsittelyä. Direktiivin tavoite on yhteiskunnan toiminnan kannalta kriittisten organisaatioiden kyberturvallisuuden varmistaminen huomioiden kaikki kyberturvallisuutta uhkaavat riskit.

Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriöntietokyvyn parantamisesta (310/2025) velvoittaa kriittisiä toimijoita seuraaviin toimenpiteisiin:

1. Riskiarvioinnin teko
2. Häiriönsietokykyä koskevan suunnitelman luominen
3. Häiriönsietokyvyn varmistaminen
4. Poikkeamia koskevan menettelyn kehittäminen

VESFY-hanke kytkeytyy erityisesti häiriönsietokykyä koskevaan suunnitelmaan sekä häiriönsietokyvyn varmistamiseen antamalla vesihuollon ammattilaisille konkreettisia ohjeita ja työkaluja vesihuoltolaitosten fyysisen turvallisuuden kehittämiseen. Lain mukaan kohdassa 2 mainitun häiriönsietokykyä koskevan suunnitelman tulee sisältää selostus tilojen ja niissä sijaitsevan infrastruktuurin suojaamisesta, kuten aidan asentamisesta, esteiden pystyttämisestä, ilmaisulaitteista ja kulunvalvonnasta sekä muusta fyysisestä suojaamisesta. Lisäksi toimenpiteet poikkeamien seurausten hallinnoimiseksi sekä häiriötilanteisiin vastaamiseksi, torjumiseksi ja lieventämiseksi.

Avainhallintaa ei määritä suoraan mikään yksittäinen laki, vaan siihen liittyvät käytännöt perustuvat vakiintuneisiin menettelytapoihin sekä lukitusliikkeiden tuottamiin ohjeisiin. Kansallisia ohjeistavia dokumentteja ovat Finanssialan tuottamat Avainturvallisuusohje sekä Rakenteelliset murtosuojausohjeet.

Vaikka yllä kuvatut lakivelvoitteet koskevat kriittiseksi toimijaksi virallisesti tunnistettuja ja nimettyjä organisaatioita, ne tukevat myös alan pienempien toimijoiden jatkuvuudenhallintaa. Näin ollen myös pienten vesihuoltolaitosten kannattaa huomioida yllä mainitut toimenpiteet omassa toiminnassaan.

1.3 HANKKEEN RAJAUKSET

Vuonna 2024 toteutetussa kyberturvallisuuteen keskittyneessä VESKY-hankkeessa kuvattiin vesihuoltoa seuraavasti: *”Vesihuolto määritellään kriittiseksi infrastruktuuriksi. Se nostaa toimintavarmuusvaatimuksen kovemmaksi kuin pelkkä murtoriskianalyysi määrittäisi.” (4.) Vesihuollon murtoriskeissä kannattaa painottaa enemmän seurausten vakavuutta kuin todennäköisyyttä, sillä vesihuolto on osa kriittistä infrastruktuuria, jossa toimintavarmuus on keskeistä. (20.)”*

Vesihuoltolaitokset koostuvat useista rakennuksista ja rakenteista, joissa vesihuoltoon liittyvät prosessit toimivat tai joita ne suojaavat. Laitokset eroavat toisistaan merkittävästi, mikä vaikuttaa suojausratkaisujen valintaan. Keskeistä on löytää tasapaino, jossa kunkin laitoksen yksilöllisiin tarpeisiin sovitetaan ratkaisut, jotka turvaavat sen kriittisimmät kohteet ja prosessit sekä ovat taloudellisesti järkeviä ja kustannustehokkaita. Tämä opas painottuu vesihuollon maanpäällisiin kohteisiin ja niiden fyysisen turvallisuuden toteuttamiseen normaalioloissa ja normaaliolojen häiriötilanteissa. Luvussa 6 otetaan kantaa varautumiseen poikkeusoloja varten.

Toinen keskeinen rajaus on keskittyminen vain rakenteelliseen ja turvatekniikalla toteutettavaan valvontaan sekä näihin liittyviin hallinnollisiin huomioihin ja palveluihin. Kyberturvallisuus liittyy erottamattomasti vesihuoltoalan toimintaan ja menee osin päällekkäin fyysisen turvallisuuden teemojen kanssa. Vesihuoltoalan kyberturvallisuutta on käsitelty syvemmin VESKY-hankkeessa, jonka tavoitteena oli vesihuoltolaitosten konkreettisen kyberturvallisuusosaamisen kehittäminen sekä vesihuoltolaitoksia yleisesti hyödyttävien malliprosessien ja -dokumenttien luominen. Siksi VESFY-hanke keskittyy mm. sellaisiin fyysisen turvallisuuden suojauskeinoihin, jotka suojaavat kyberturvallisuuteen liittyvää laitteistoa tai järjestelmän liityntäpisteitä, joiden kautta voi päästä käsiksi tietoverkkoihin.

Suojauskeinojen ohella on välttämätöntä käsitellä hallinnollista ulottuvuutta eli sitä, miten varmistetaan, että fyysisen turvallisuuden suojauskeinoja käytetään tarkoituksenmukaisella tavalla. Aihe kytkeytyy turvallisuusjohtamiseen, jota on käsitelty kattavasti Vesihuoltolaitosyhdistyksen julkaisussa *"Turvallisuusjohtaminen vesihuoltolaitoksilla"*. Julkaisu sisältää tietoa turvallisuusjohtamisen perusteista ja ehdotuksia toteutustavoista nimenomaan vesihuoltoympäristössä. Näin ollen tässä oppaassa kuvataan turvallisuusjohtamiseen liittyviä prosesseja ja käyttäjien roolia vain siltä osin, kuin ne liittyvät fyysiseen suojaukseen ja erilaisten suojausratkaisujen käyttöön.

1.4 HANKKEEN KOHDERYHMÄT

Oppaan tarkoitus on auttaa vesihuoltoalan toimijoita parantamaan fyysistä turvallisuutta omissa kohteissaan. Ensimmäinen ja tärkein askel on arvioida, mitkä rakennukset, laitteet ja toiminnot ovat kriittisiä juuri oman laitoksen toiminnan turvaamiseksi. Samalla on tärkeää arvioida, millä tavoin näiden kohteiden suojaamista voidaan parantaa käytettävissä olevien resurssien puitteissa – kuten budjetin ja henkilöstön. Kun nämä perusasiat ovat selvillä, oppaasta löytyy ratkaisuja, joita voi soveltaa omiin tarpeisiin.

Oppaan keskeisimpiä kohderyhmiä ovat erityisesti seuraavat vesihuoltoalan ammattilaiset sekä hankesuunnitteluun osallistuvat ulkoiset sidosryhmät:

- Vesihuoltolaitosten ylin johto
- Vesihuoltolaitosten turvallisuusvastaavat
- Saneeraus- ja uudiskohteiden projektipäälliköt
- Saneeraus- ja uudiskohteiden suunnittelijat

Opas pyrkii tarjoamaan selkeän kuvauksen erilaisten turvallisuusrakenteiden ja -ratkaisujen merkityksestä ja tarpeellisuudesta koko laitoksen toiminnan turvaamisen kannalta. Tämä tukee ylimmän johdon turvallisuutta koskevien tavoitteiden määrittelyä ja linjausta, joihin erilaiset turvallisuuden kehittämishankkeet pohjautuvat.

Opas tukee hankesuunnittelua tarjoamalla konkreettisia suosituksia ja selkeitä työvälineitä niin turvallisuusasioista vastaaville kuin projektipäälliköille. Opas auttaa arvioimaan, kuljetaanko kehityksessä oikeaan suuntaan, tunnistamaan keskeiset kehityskohteet ja mahdollisuudet sekä kohdentamaan resurssit tehokkaasti. Lisäksi se ohjaa arvioimaan, mistä on suositeltavaa aloittaa kehitystoimet ja mikä on fyysisen turvallisuuden suojauskeinojen yleinen minimitaso vesihuoltoalalla. Tavoitteena on parantaa suunnittelijoiden ja koko vesihuoltoalan osaamista turvallisuusasioissa.

Näiden tavoitteiden lisäksi oppaan suunnittelussa on huomioitu sen käytettävyys ja oppaasta on pyritty luomaan selkeä, helposti arjessa käytettävä ja käytännön esimerkkejä sisältävä.

1.5 TERMIT JA MÄÄRITELMÄT

Tässä luvussa käydään läpi kaikki keskeiset termit. Yhtäläisen termistön käyttö helpottaa turvallisuusasioista keskustelemista sisäisesti, muiden vesihuoltoalan toimijoiden kesken sekä sidosryhmien, kuten urakoitsijoiden, kanssa. Termit ovat aakkosjärjestyksessä.

Aluesuojaus
Kohdetta ympäröivän maa-alueen (ja ilma-alueen) suojaaminen

ATV-varaus
”Ajoneuvojen ja työkoneiden varaaminen” – Järjestelmä, jolla viranomaisella on lakisääteinen oikeus ottaa itselleen kalustoa poikkeusoloissa, mutta huomioiden kuitenkin siviiliyhteiskunnan tarpeet siten, ettei kriittiset toiminnot häiriinny liikaa.

CPTED-malli
Crime Prevention Through Environmental Design -periaate, jossa ympäristön suunnittelulla vähennetään rikosriskejä ja lisätään turvallisuutta.

End of Life (EOL)
Tällä tarkoitetaan vaihetta, jossa jokin tuote, järjestelmä tai palvelu on saavuttamassa käyttöikänsä loppua ja sen toimittaja lopettaa tuotannon, myynnin ja käytössä olevien versioiden teknisen tuen tarjoamisen.

GAP-analyysi
Menetelmä, jolla verrataan nykytilaa ja tavoitetilaa, jotta voidaan tunnistaa puutteet ja kehitystarpeet.

Hallinnollinen turvallisuus
Kattaa organisaation toimintatavat, ohjeet ja prosessit, joilla varmistetaan tietojen ja toiminnan suojaaminen hallinnollisin keinoin.

Häiriötilanne
Uhka tai tapahtuma, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. Häiriötilanteita voi esiintyä niin normaalioloissa kuin poikkeusoloissakin. Häiriötilanne voi koskea esimerkiksi koko valtakuntaa tai olla alueellinen tai paikallinen. Häiriötilanne voi myös liittyä ainoastaan johonkin toimintoon.

Huoltovarmuus
Toiminta, jonka tarkoituksena on turvata väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämätön tuotanto, palvelut ja infrastruktuuri vakavien häiriötilanteiden ja poikkeusolojen varalta.

Huoltovarmuuskriittinen organisaatio on organisaatio, joka on erityisen merkittävä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Huoltovarmuuskriittinen organisaatio voi olla yritys tai muu organisaatio.

Jatkuvuuden hallinta
Huoltovarmuutta parantava – ylimmän johdon hyväksymä – organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle.

Kehäsuojausmalli
Turvallisuusratkaisu, jossa alue suojataan useilla toisiaan täydentävillä suojausvyöhykkeillä ja -ratkaisuilla (ulkokehäsuojaus, aluesuojaus, kuorisuojaus, tilasuojaus ja kohdesuojaus).

Kohdesuojaus
Kriittisimpien toimintojen tai tilojen suojaaminen.

Kriittinen infrastruktuuri
Perusrakenteita, palveluja ja niihin liittyviä toimintoja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Vesihuolto on osa kriittistä infrastruktuuria.

Kriittinen palvelu
Palveluja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Kriittisiin palveluihin kuuluvat elintarvikehuoltoa, terveydenhuoltoa, peruspalveluja, teollisuutta ja sotilaallista maanpuolustusta tukevat palvelut.

Kriittinen tuotanto
Välttämätöntä tuotantoa yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Kriittiseen tuotantoon kuuluu mm. elintarvikehuollolle, terveydenhuollolle, peruspalveluille, teollisuudelle ja sotilaalliselle maanpuolustukselle välttämätön tuotanto.

Kuorisuojaus
Kohteen ulkokuoren eli seinien, katon, ikkunoiden, ovien ja luukkujen suojaaminen.

Kulunhallinta
Prosessi ja järjestelmät, joilla hallitaan ihmisten liikkumista tilojen sisällä, esimerkiksi ovien ja kulkureittien käyttöoikeuksia. Voidaan toteuttaa esimerkiksi kulunvalvontajärjestelmän tai elektromekaanisen lukitusjärjestelmän avulla.

Kyberfyysinen turvallisuus
Kattaa sekä perinteisen toimitilaturvallisuuden että kyberturvallisuuden.

Mekaanisen lukituksen patenttisuojaus
Lukitusmekanismin rakenteen ja toiminnallisten ratkaisujen oikeudellinen suojaaminen määräajaksi, jonka jälkeen suoja raukeaa ja ratkaisu voidaan valmistaa tai kopioida ilman lupaa.

Normaaliolot
Yhteiskunnan pääsääntöinen tila, jossa yhteiskunnan elintärkeät toiminnot voidaan turvata ilman, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö. Normaalioloissa rakennettavat järjestelmät ja muut toimenpiteet luovat perustan toiminnalle häiriötilanteissa ja poikkeusoloissa.

Poikkeusolot
Valmiuslaissa tarkoitettu yhteiskunnan tila, jossa on niin paljon tai niin vakavia häiriöitä tai uhkia, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö. Poikkeusolojen vallitsemisen toteaa valtioneuvosto yhteistoiminnassa tasavallan presidentin kanssa.

Pääsynhallinta
Menetelmät ja teknologiat, joilla määritellään ja valvotaan, kenellä on oikeus päästä tiettyyn tilaan tai tiettyyn järjestelmään.

Rakenteellinen turvallisuus
Fyysiset rakenteet ja ratkaisut, kuten seinät, aidat, portit ja lukot, jotka estävät tai hidastavat luvattoman pääsyn suojattavaan kohteeseen.

Riski
Kielteisen seikan tai tapahtuman (uhka tai vaara) todennäköisyyden ja vaikutusten yhdistelmä.

Riskianalyysi
Toiminta, jossa tunnistetaan riskit ja arvioidaan vahinkotapahtuman todennäköisyys sekä odotettavissa olevat vahingot.

Riskienhallinta
Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. Riskienhallinnan keinoja ovat riskin välttäminen, siirtäminen, pienentäminen jakamalla ja vahingontorjunnalla sekä riskin ottaminen. Vesihuoltolaki asettaa lakisääteisen velvoitteen laatia valmiussuunnitelma, johon riskienhallinta kuuluu tärkeänä osana. Vesihuoltolaissa 15 a §: "suunnitelma häiriötilanteisiin varautumisesta". Valmiussuunnitteluvelvoite tulee valmiuslain 12 §:stä. Se kuitenkin koskee nimenomaisesti valtion liikelaitoksia, hyvinvointialueita, hyvinvointiyhtymiä sekä kuntia ja kuntayhtymiä. Yhtiömuodossa toimivia laitoksia se ei koske.

Tilasuojaus
Kohteen sisätilojen suojaaminen eri kriittisyysluokkien mukaisesti, joille määritellään omat suojaustoimenpiteet.

Turvallisuus
Turvallisuus voidaan jakaa kahteen kategoriaan: safety ja security.

- Safety:
  - ”Pehmeä” turvallisuus, joka ei vaarannu tarkoituksellisen toiminnan vuoksi vaan esimerkiksi tapaturmien, onnettomuuksien tai virheiden vuoksi (kuten työturvallisuus, tuotteiden käyttöturvallisuus, onnettomuuksien ehkäisy)
- Security
  - ”Kova” turvallisuus, joka liittyy tarkoitukselliselta vahingoittavalta toiminnalta suojautumiseen (kuten rikollinen toiminta, sabotaasi).
  - Tässä oppaassa turvallisuudella tarkoitetaan security-turvallisuutta

Turvallisuuskulttuuri
Turvallisuuskulttuurilla tarkoitetaan sitä, minkälaisia asenteita, ajatuksia ja toimenpiteitä yksittäisessä organisaatiossa on kohdistuen turvallisuuteen ja turvallisuustoimintaan.

Turvatekniikka
Teknologiset järjestelmät, kuten kameravalvonta, kulunvalvonta ja hälytysjärjestelmät, jotka tukevat turvallisuuden hallintaa.

Turvavarastointi
Varmuusvarastointia (materiaalivarastot), josta vesihuoltolaitos huolehtii vapaaehtoisesti turvatakseen oman toimintansa häiriötilanteissa ja poikkeusoloissa.

Uhka
Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Uhka eroaa vaarasta siten, että uhka on epävarmempi kehityskulku ja vaara puolestaan käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävä asia.

(Ulko)kehäsuojaus
Kohteen raja-alueen ja aitalinjojen suojaaminen.

Vaara
Hyvin todennäköisesti toteutuva tai jo toteutunut, parhaillaan vaikuttava haitallinen tapahtuma tai kehityskulku.

Varautuminen
Toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdolliset poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa.

Valmius
Tila, joka on saavutettu varautumisella ja jossa kyetään vastaamaan erilaisiin uhkiin.

VAP-henkilö
Asevelvollinen tai siviilipalvelusvelvollinen, joka on virka- tai työtehtävänsä vuoksi varattu poikkeusoloissa muuhun kuin puolustusvoimien palvelukseen.

1.6 OPPAAN KÄYTTÖ

Opas on tarkoitettu käytettäväksi tilanteissa, joissa
a) vesihuoltolaitoksen turvallisuusvastaava haluaa arvioida fyysisen turvallisuuden kehitystarpeita,
b) suunnitellaan laitoksen tai sen yksittäisen kohteen saneerausta
c) suunnitellaan kokonaan uusi tuotantolaitos tai sen osatoiminto.

Opas toimii työkaluna organisaatiossa turvallisuustyötä tekevälle henkilölle ja sen pohjalta laaditaan organisaatiokohtainen fyysisen turvallisuuden suunnitelma. Oppaan teossa on huomioitu, että monesti laitosten turvallisuustyötä tekee yksittäinen henkilö oman työnsä ohessa, eikä hänellä välttämättä ole erityistä turvallisuusosaamista. Tätä ajatellen hallinnollisen turvallisuuden ja turvallisuuden kehitystyön perusteita ja merkityksiä on kuvattu **luvussa 2**.

Oppaan tueksi on työkalu, jonka avulla yksittäisen vesihuoltolaitoksen on mahdollista arvioida oman laitoksensa tai yksittäisten arvioitavien kohteiden kriittisyysluokka, tunnistaa oman toimintansa kannalta kriittisimmät tilat, laitteet ja prosessit sekä niiden suojauksen nykytila ja verrata nykytilaa suosituksiin. Työkalua voi hyödyntää joko sellaisenaan tai osiltaan soveltaen sitä omiin tarkoituksiinsa fyysisen turvallisuuden kehittämistyökaluna. Työkalu on **liitteenä 6**.

Opas antaa perustietoa fyysisen turvallisuuden perusperiaatteista sekä erilaisista toteutustavoista eri kokoisissa laitoksissa. Se on tarkoitettu toimimaan yhdessä liitteiden ja työkalun kanssa, mutta opasta voi hyödyntää sellaisenaankin.

Käytä opasta näin:

Jos turvallisuustyö ei ole entuudestaan tuttu aihepiiri:
1. Aloita luvusta 2.
    a. Tee vesihuoltolaitoksen nykytilan esiarviointi (pohja **liitteessä 5**)
    b. Tämän jälkeen käytössäsi on keskeiset perustiedot, joita voit hyödyntää oppaaseen tutustuessasi.
2. Tee kohteen kriittisyyden arviointi oppaan tueksi tehdyn työkalun avulla (**liite 6**).

   a. Arvioinnin lopputuloksena saat yhteenvedon, josta näet arvioimasi kohteen kriittisyyden, suojauksen nykytilan ja suosituksen siitä, minkälaisia suojauskeinoja kyseisen tyyppiseen kohteeseen yleensä suositellaan.
3. Etsi oppaasta ratkaisuja havaitsemiisi puutteisiin.

Jos turvallisuustyö on sinulle tuttua:
1. Voit halutessasi hyödyntää organisaation nykytilan esiarviointia (pohja liitteessä 5) tai aloittaa suoraan kohdasta 2 (alla).
2. Tee kohteen kriittisyyden arviointi oppaan tueksi tehdyn työkalun avulla (**liite 6**).
   a. Arvioinnin lopputuloksena saat yhteenvedon, josta näet arvioimasi kohteen kriittisyyden, suojauksen nykytilan ja suosituksen siitä, minkälaisia suojauskeinoja kyseisen tyyppiseen kohteeseen yleensä suositellaan.
3. Etsi oppaasta ratkaisuja havaitsemiisi puutteisiin.

2 HALLINNOLLISEN TURVALLISUUDEN TOTEUTTAMINEN

2.1 TURVALLISUUSJOHTAMISEN JA TURVALLISUUDEN KEHITTÄMISTYÖN PERUSTEET

Vesihuoltolaitosyhdistyksen julkaisussa *”Turvallisuusjohtaminen vesihuoltolaitoksilla”* todetaan seuraavaa:

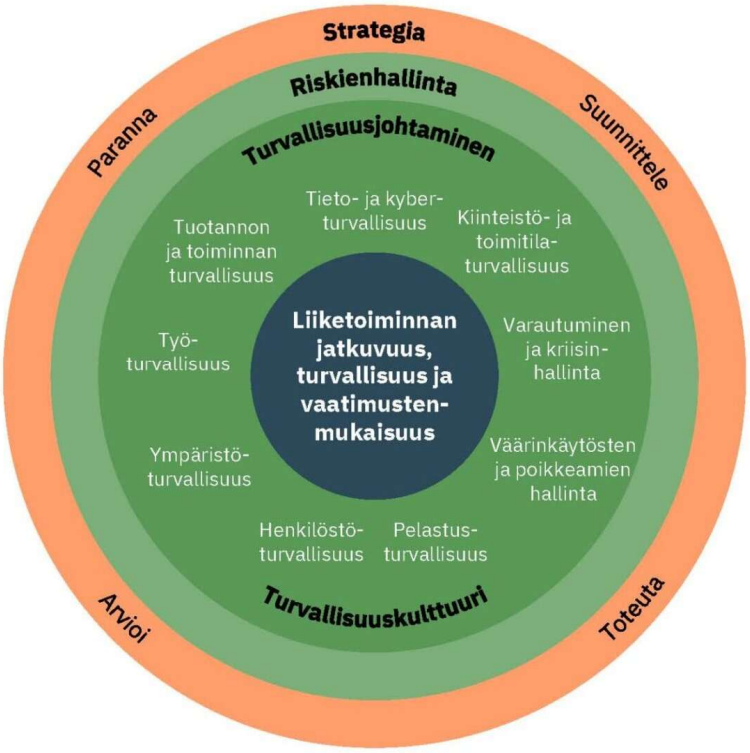
”*Yhtenäinen turvallisuusjohtamisjärjestelmä antaa mahdollisuuden kehittää ja parantaa vesihuoltolaitosten nykyisiä toimintatapoja ja yhtenäistää vesihuoltolaitosten turvallisuuskulttuuria. Vaikuttamalla systemaattisesti häiriötilanteiden syntymekanismeihin voidaan riskejä poistaa, häiriötilanteita ehkäistä ja syntyneitä erityistilanteita hallita nykyistä tehokkaammin. Vesihuoltolaitokset voivat ohjeistuksen perusteella painottaa kehittämistään niihin osa-alueisiin, joissa havaitsevat eniten puutteita omassa toimintamallissaan.”*

Turvallisuusjohtamisen voidaankin tiivistää olevan organisaation fyysiseen turvallisuuteen liittyen asioiden kartoitusta, kehitystä ja toteutumisen valvontaa. Turvallisuuden kehitystyössä on tiivistettynä kyse siitä, miten pidetään organisaation rakennukset, omaisuus, tärkeä tieto ja siellä työskentelevät ihmiset turvassa. Kaiken toiminnan pohjalla ovat tietyt perusasiat:

- Mitä täytyy tehdä, että oman organisaation tärkeimmät toiminnot voivat toteutua mahdollisimman häiriöttömästi tilanteessa kuin tilanteessa?
- Mitkä ovat oman organisaation tärkeimmät suojattavat asiat?
- Minkälaisia uhkatekijöitä niihin voi kohdistua juuri siinä ympäristössä (maantieteellinen sijainti, sosiaalinen ympäristö), jossa organisaatio toimii?

Elinkeinoelämän keskusliiton luoma yritysturvallisuusmalli (kuva 1) auttaa hahmottamaan yritysten turvallisuuskenttää ja sen eri osa-alueita. Yritysturvallisuusmalli on tarkoitettu kaiken kokoisille organisaatioille ja perustuu ajatukseen siitä, että turvallisuusjohtaminen on osa normaalia yrityksen johtamista, ei siitä irrallinen kokonaisuus.

Mallin ytimessä on yrityksen toiminnan jatkuvuuden, turvallisuuden ja vaatimustenmukaisuuden varmistaminen kaikissa tilanteissa. Sitä ympäröivät turvallisuuden eri osa-alueet. Osa-alueet eivät ole toisistaan irrallisia kokonaisuuksia vaan usein ne limittyvät keskenään. Osa-alueiden merkitys yrityksille riippuu niiden toimialasta ja toiminnan luonteesta ja keskeistä on tunnistaa siitä omalle organisaatiolle tärkeimmät osa-alueet. Osa-alueita hallinnoidaan turvallisuusjohtamisen ja turvallisuuskulttuurin kehittämisen kautta. Riskienhallinnan avulla voidaan tunnistaa oman organisaation tärkeimpiin osa-alueisiin liittyviä riskejä ja uloimmalla kehällä kulkee strateginen toiminnan jatkuva kehittäminen.



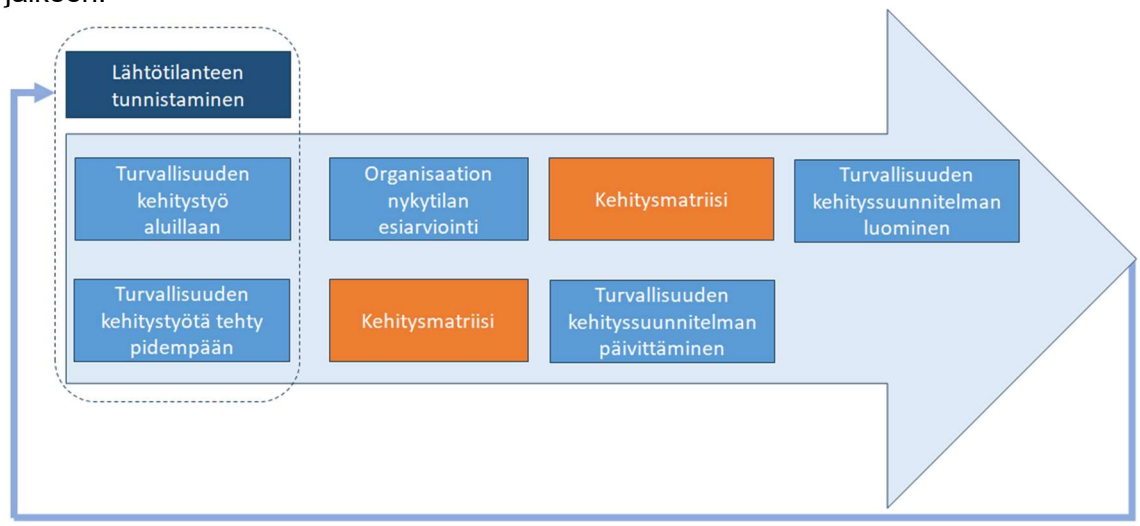
Kuva 1: Elinkeinoelämän keskusliiton kehittämä yritysturvallisuusmalli

Yritysturvallisuuden kokonaisuutta voi hahmottaa myös Elinkeinoelämän keskusliiton tuottaman yritysturvallisuusmatriisin avulla (kuva 2). Matriisi kuvaa sitä, mitä toiminnallisuuksia turvallisuuden kehittämiseen liittyy (turvallisuusjohtaminen ja -viestintä, sidosryhmäyhteistyö, varmentaminen ja auditointi, jatkuva kehittäminen) ja miten ne läpäisevät organisaation perustan (henkilöstö, tuotanto ja toiminta, tieto, toimitilat, ympäristö). Kuten yritysturvallisuusmallissa, kaiken pohjalla on riskienhallinta. Organisaation liiketoimintamalli ja strategia luovat rajat ja tavoitteet sille, mihin teemoihin turvallisuuden kehittämisessä keskitytään.

Kuva 2: Elinkeinoelämän keskusliiton kehittämä yritysturvallisuusmatriisi

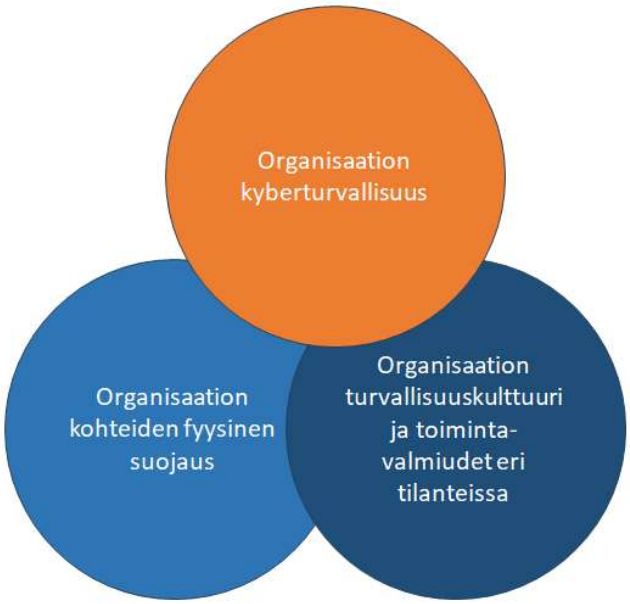
Organisaatioilla on erilaisia mahdollisuuksia ja resursseja turvallisuuden kehittämiseen. Yhdessä organisaatiossa on henkilö, jonka päätyö on turvallisuusasioiden hoitaminen,

toisessa taas yhdellä henkilöllä on monta erilaista vastuualuetta, joista yksi on turvallisuus. Tämä opas pyrkii tarjoamaan tietoa ja vaihtoehtoja koko tämän skaalan mitalta. Tärkeintä onkin tunnistaa oman organisaation tilanne, josta turvallisuuden kehittämistyöhön lähdetään ja etsiä oppaasta omaan tarpeeseen ja budjettiin sopivia ratkaisuja. Kuvassa 3 esitetään, miten opasta kannattaa käyttää nykytilan tunnistamisen jälkeen. On tärkeää huomioida, että fyysisen turvallisuuden ylläpito ei ole kertaluontoinen projekti vaan jatkuva prosessi. Kuvassa 3 tätä kuvaa sininen nuoli, joka johtaa takaisin lähtötilanteen tunnistamiseen turvallisuuden kehityssuunnitelman luomisen/päivittämisen jälkeen.



Kuva 3: Oppaan käyttö nykytilan tunnistamisen jälkeen

Mikäli organisaation turvallisuustyö on aivan alussa, kannattaa aloittaa vastaamalla liitteessä 5 esitettyihin kysymyksiin. Lopputulos on yhteenveto organisaation turvallisuuden peruselementtien nykytilanteesta (kuva 4) ja se toimii pohjana turvallisuuden kehityssuunnitelmalle.



Kuva 4: Turvallisuuden peruselementit

Turvallisuuden kehitystyö perustuu kohdekohtaiseen riskienarviointiin ja turvallisuuskulttuurin tason arviointiin.

Kohteen riskienarvioinnissa on tarkoitus vastata seuraaviin kysymyksiin:

- Minkälaisessa ympäristössä laitos toimii, minkälaisia asiakkaita se palvelee?
- Mitkä ovat laitoksen toiminnassa sellaisia laitteita tai toimintoja, joiden häiriintymisellä voidaan lamauttaa laitoksen toiminta tai aiheuttaa sille merkittävää haittaa (rahallinen, materiaalinen, terveydellinen yms.)?
- Vesilaitoskokonaisuuden kaikkien rakennusten ja rakennelmien suojaaminen vaatii suuria taloudellisia panostuksia eikä kaikkea useinkaan ole mahdollista tehdä kerralla.
    - Mitkä siis ovat kaikkein kriittisimmät pisteet, joiden suojaamiseen panostetaan eniten ja jotka suojataan ensimmäisenä?
    - Mitkä kohteet tulevat niiden jälkeen?

Kriittisiä kohteita määrittäessä on hyvä pitää mielessä fyysisen suojauksen tarkoituksen ydin. Kohteen fyysisellä suojaamisella pyritään suojaamaan organisaation tahtotilan tai toiminnan kannalta tärkeitä arvoja erinäisiltä uhilta. Siten kohteen suojaamisen perustana on suojattavien arvojen tunnistaminen – mikä meille on tärkeää? Tyypillisiä suojattavia arvoja ovat esimerkiksi jokapäiväisen toiminnan mahdollistava työntekijöiden terveys, toiminnan häiriöttömyyden kannalta kriittiset laitteet, järjestelmät ja prosessit, organisaation vakavaraisuuteen vaikuttava omaisuus, salassa pidettävät tietoaineistot sekä organisaation maine (kuva 5).

Kuva 5 Organisaation suojattavat arvot

Lisätietoa:

- Riskienarviointia on käsitelty yksityiskohtaisemmin luvussa 3.
- Erilaisia keinoja organisaation arvojen suojaamiseksi esitetty luvussa 4.
- Oppaan tueksi tehty työkalu (liite 6), joka auttaa arvioimaan oman vesihuoltolaitoksen kohteiden kriittisyyttä ja antaa yksityiskohtaisia suosituksia suojauskeinoista.

Turvallisuuskulttuurin kehittäminen, työntekijöiden turvallisuusosaamisen ja organisaation turvallisuuskäytäntöjen kehittäminen on hyvä ensimmäinen askel. Paras hyöty saadaan, kun korkean tason turvallisuuskulttuurin organisaatioon lisätään kohdetta parhaiten palvelevat suojauskeinot ja käyttäjät perehdytetään niiden asianmukaiseen käyttöön. Keskeistä on pyrkiä luomaan sellainen asenneilmasto, jossa virheiden esiin tuominen on turvallista. Virheistä kertomiseen suhtaudutaan rohkaisevasti ja yksittäisen työntekijän rankaisemisen sijaan keskitytään syihin, jotka mahdollistivat virheen synnyn. Avoin ja rehellinen keskustelukulttuuri on edellytys sille, että tieto ja havainnot liikkuvat työntekijöiden ja ylimmän johdon välillä.

Tähän sisältyy se, miten turvallisuusasioita pidetään organisaatiossa esillä. Turvallisuustyön organisointi, kuten käytännöt ja dokumentaatio. Jos jotain sovitaan, miten varmistetaan, että siitä pidetään kiinni? Nähdäänkö turvallisuus asiana, jota joku muu toteuttaa vai asiana, joka syntyy jokaisen arkisesta toiminnasta?

Esimerkiksi järjestelmällisen turvallisuushavaintojen kirjanpidon avulla saadaan kokonaiskuva organisaatiolle tyypillisistä riskeistä ja puutteista sekä turvallisuusympäristöstä. Turvallisuushavaintojen määrä ja laatu ovat myös yksi ilmentymä organisaation kyvystä havaita ja tunnistaa poikkeamia, turvallisuusosaamisen tasosta sekä yleisesti turvallisuuskulttuurista. Vähäinen turvallisuushavaintojen määrä voi merkitä sitä, että kaikki on kunnossa – tai sitä että tietynlaisiin asioihin ei osata kiinnittää huomiota, havainnoista ei ilmoiteta eteenpäin tai ajatellaan, että joku muu hoitaa. Tärkeää onkin selvittää, mistä tilanne johtuu, jotta voidaan valita oikeat korjauskeinot. Näin turvallisuushavaintojen myötä saatu tieto toimii pohjana turvallisuuden kehittämishankkeiden määrittelylle. Havaintojen tilastointi antaa myös tarkkaa tietoa, jota on mahdollista hyödyntää hakiessa rahoitusta kehityshankkeelle.

Eri henkilöstöryhmien osalta turvallisuuden osa-alueiden vastuiden painotuksissa on roolin mukaisia eroja, mutta viime kädessä vastuu turvallisuuden toteuttamisesta on jokaisella vesihuolto-organisaatioon kuuluvalla jäsenellä sekä sidosryhmillä.

Seuraavaksi käydään läpi organisaation eri roolien vastuualueita. Turvallisuus on organisaation ydintoimintaa tukeva toiminto. On kuitenkin tärkeää huomata, että onnistunut turvallisuuden kehitystyö vaatii aina sekä tekijöitä ja taloudellista panostusta. Siksi kaikelle turvallisuustyölle tulee aina olla ylimmän johdon tuki.

- **Ylimmän johdon** tulee ymmärtää fyysisen turvallisuuden ja sen kehittämisen merkitys, olla sitoutunut turvallisuuden kehittämiseen, määritellä turvallisuustyön tavoitteet, linjata miten oman vesihuollon turvallisuutta kehitetään ja antaa riittävät resurssit kehitystyöhön. Suhtautuminen turvallisuuteen lähtee ylimmästä johdosta ja läpäisee koko organisaation.
- **Keskijohdon** vastuu on ylimmän johdon linjausten noudattaminen, turvallisuusperiaatteiden sisäistäminen, turvallisuuden toimenpiteiden toteuttaminen sekä toimenpiteiden toteutumisen valvominen.
- **Työntekijöiden** vastuu on sisäistää ylimmän johdon määrittämät turvallisuusperiaatteet, noudattaa annettua turvallisuusohjeistusta, ymmärtää oman toimintansa merkitys vesihuollon turvallisuuden kannalta ja osallistua aktiivisesti organisaation turvallisuuden kehittämiseen.

2.2 HALLINNOLLISEN TURVALLISUUDEN MERKITYS

Hallinnollisen turvallisuuden merkitys on huomioitu jo standarditasolla.
ISO 24596:2024-standardi jaottelee vesihuoltoinfrastruktuurin suojauksen vahvistamistoimenpiteet kahteen kategoriaan:

- sähköiset ja ei-sähköiset
- henkilöstö- ja organisatoriset

Kaikkien näihin kategorioihin kuuluvien toimenpiteiden tarkoituksena on vaikeuttaa tahallista tai tahatonta palvelun häirintää ja laadun heikentämistä. Samaisen standardin mukaan fyysisen turvallisuuden ylläpito edellyttää fyysisiä, henkilöstöön liittyviä sekä organisatorisia toimenpiteitä, joilla pyritään pienentämään riskejä hyväksyttävälle tasolle.

Lisäksi ISO 24596:2024-standardissa todetaan, että erityiset riskienhallintatoimenpiteet tulisi asettaa tärkeysjärjestykseen siten, että etusijalla ovat toimenpiteet, jotka osoittavat suurta luotettavuutta ja toimintavarmuutta (esimerkiksi vähäinen virheellisten hälytysten määrä). Yksittäisten kohteiden tehokkain suojaus saavutetaan fyysisten, henkilöstöön liittyvien ja organisatoristen toimenpiteiden kokonaisvaltaisella yhdistelmällä.

Hallinnollinen turva tarkoittaa käytännössä sen määrittelyä, miten turvallisuutta organisaatiossa toteutetaan ja miten erilaiset vastuut jakautuvat. Hallinnollisen turvan tasolla määritellään perusperiaatteet, joihin perustuen luodaan ohjeita, koulutuksia ja käytäntöjä sekä valitaan erilaisia teknisiä järjestelmiä. Perusperiaatteet ovat samat, oli kyseessä turvatekninen järjestelmä, organisaation fyysiset rakenteet tai organisaation arkaluontoinen tieto.

1. Tunnistetaan kriittisimmät/arkaluontoisimmat arvot.
2. Määritellään
    a. kenellä tulee olla niihin pääsy
    b. millä perusteilla (huomioiden sijaisjärjestelyt)
    c. minkälaisessa laajuudessa.
3. Rajataan pääsy vain näille henkilöille.

Nämä kolme kohtaa toistuvat seuraavissa alaluvuissa, toteutuen hieman eri tavoin asiayhteydestä riippuen.

2.3 TURVALLISUUSPOLITIIKAN MERKITYS

Tässä kappaleessa käydään läpi organisaatiokohtaisen turvallisuuspolitiikan merkitystä sekä kuvataan siihen liittyvien vastuiden jakautumista koskien turvallisuuspolitiikan luomista, jalkauttamista, käyttöä, käytön valvontaa sekä ylläpitoa ja hallinnointia. Lisäksi tässä luvussa kuvataan erilaisiin yksittäisiin järjestelmiin liittyviä vastuita ja rooleja.

Turvallisuuspolitiikka

- kuvastaa organisaation johdon tahtotilaa
- kuvaa organisaation turvallisuusjohtamisen periaatteet
- mahdollistaa turvallisuustoiminnan hallinnoinnin
- luo pohjan turvallisuusjohtamisen toimintamallin kehittämiselle.

Näin ollen turvallisuuspolitiikan tulee sisältää ainakin

- Turvallisuustoiminnan organisaatio ja siihen kuuluvien turvallisuusvastuut, toimivallat ja resurssit
- Turvallisuuspolitiikan omistaja, jonka vastuulla on dokumentin pitäminen ajan tasalla
- Kuvaus siitä, mille tahoille turvallisuuspolitiikka jaetaan milläkin laajuudella.
    - *Esim. Turvallisuuspolitiikan arkaluontoisimmat tiedot jaetaan rajatun vastaanottajaryhmän kesken, turvallisuuspolitiikasta irrotetaan yleistasoinen osio laajemmalle kohderyhmälle jaettavaksi.*
- Turvallisuustoiminnan tavoitteet ja päämäärä
- Turvallisuuden vähimmäistason määritelmä
- Toimintasuunnitelma tavoitteiden saavuttamiseksi vastuineen
    - toimenpiteet ja aikataulu
    - koulutus
    - suunnitelman toteutumisen seuranta
- Kuvaus siitä, miten politiikkaa koskevia päivitystarpeita seurataan ja käsitellään
    - Prosessi, jolla periaatteisiin kohdistuvat muutokset hyväksytään
- Toimintaperiaatteet ja vastuut sellaisten tilanteiden varalta, joissa tarpeen poiketa periaatteista.
    - Ennakkoarvio tilanteista, joissa voidaan joutua poikkeamaan normaalista toimintamallista sekä mahdollisista poikkeavista toimintamalleista.
    - Vastuuhierarkian ennakkomääritelmä:
        - Kenellä organisaatiossa on lopullinen valta tehdä päätös poikkeavan toimintamallin käyttöönotosta.

    - Kenellä on vastuu tilanteen hoidosta sen jälkeen, kun on tehty päätös toimia toisin kuin periaatteissa linjataan.
- Kuvaus siitä, miten järjestelmien käyttöä seurataan ja havaittuja väärinkäytöksiä selvitetään ja miten tämä vastuu käytännössä jakautuu.
    - Teknisten vikailmoitusten käsittely ja järjestelmämuutosten koordinointi.
    - Turvallisuuspoikkeamista (security) ilmoittamisen prosessi ja kanavat.
    - Kuvauksen tulee aina perustua arvioon kulun- ja pääsynhallintaan liittyvistä yleisimmistä riskeistä juuri kyseisessä organisaatiossa.
- Kehitystoimenpiteiden suunnittelu ja toteutuksen vastuuttaminen.
    - Kulunhallintaa koskevien kehitystoimenpiteiden noudattamisen seuranta.
    - Auditointi- ja raportointikäytännöt.

Turvallisuuspolitiikka muodostaa sateenvarjon, jonka alle turvallisuuden eri osa-alueet (esimerkiksi avainhallinta, kulunhallinta ja pääsynhallinta) sijoittuvat. Tämä on visualisoitu kuvassa 6.

Kuva 6 Turvallisuuspolitiikka ja turvallisuuden osa-alueet

Alla kuvatut vastuiden määritelmät yksittäisen organisaation turvallisuuspolitiikan osalta perustuvat Vesihuoltolaitosyhdistyksen julkaisuun ”Turvallisuusjohtaminen vesihuoltolaitoksilla”. (Vesilaitosyhdistys 2021)

Johdon vastuu

- Turvallisuuden kehitystyön mahdollistaminen osoittamalla tukea ja tarjoamalla riittävät ajalliset ja taloudelliset resurssit.
- Organisaation turvallisuuspolitiikan määrittely.
- Oman organisaation kulun- ja pääsynhallinnan periaatteiden määrittely eli kuvaus siitä, miten kulun- ja pääsynhallintaa toteutetaan käytännössä organisaatiossa.
    - Kulun- ja pääsynhallinnan periaatteiden (liite 4) hyödyntäminen pohjana organisaatiokohtaiselle työlle.

Keskijohdon vastuu

- Perehtyminen organisaation turvallisuuspolitiikkaan ja turvallisuusohjeisiin.
- Keskeisten turvallisuusohjeiden perehdyttäminen uusille työntekijöille ja kertaaminen vanhojen kanssa.
- Turvallisuusohjeiden noudattamisen valvonta.

Työntekijän vastuu

- Oman työn ja toiminnan turvallisuuden varmistaminen.
- Perehtyminen organisaation turvallisuusohjeisiin.
- Sitoutuminen organisaation turvallisuusohjeiden noudattamiseen.
- Osallistua aktiivisesti organisaation turvallisuuden kehittämiseen esimerkiksi ilmoittamalla havaitsemistaan puutteista.

Sidosryhmän vastuu

- Oman työn ja toiminnan turvallisuuden varmistaminen.
- Perehtyminen organisaation keskeisiin turvallisuusohjeisiin.
- Sitoutuminen saamiensa turvallisuusohjeiden noudattamiseen.

2.3.1 Tilojen oikeanlainen käyttö

Tilojen oikeanlaisen käytön perusta on fyysisten rakenteiden ja tilojen luokittelu.

Tilat jaotellaan tyypillisesti seuraavasti:

- voidaan sallia pääsy henkilökunnan lisäksi esimerkiksi vierailijoille,
- voidaan sallia pääsy vain henkilökunnalle sekä
- voidaan sallia pääsy vain harvoille henkilöille tiettyjen kriteerien mukaan.

Työympäristöt voidaan jaotella esimerkiksi seuraavaan neljään luokkaan:

- julkinen alue
- puolijulkinen (valvottu) alue
- hallinnollinen alue
- turva-alue

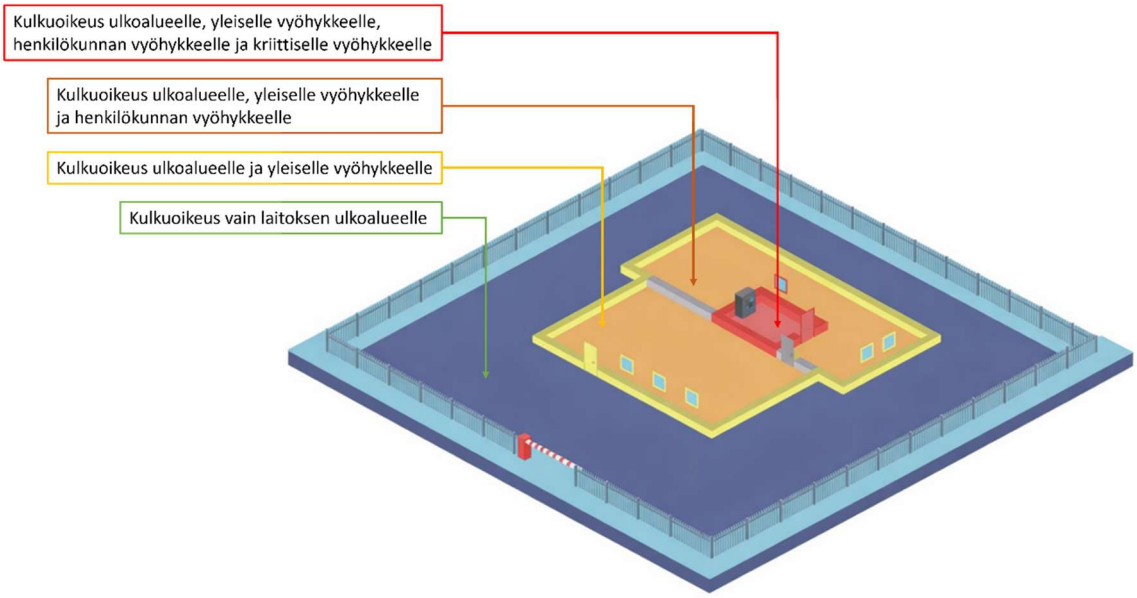
Tässä jaottelussa julkinen alue on avoin kaikille kansalaisille, puolijulkiselle alueelle saavat tulla vierailijat, hallinnollinen alue on tarkoitettu vain henkilökunnalle ja turva-alueelle pääsevät vain ne, jotka täyttävät tietyt kriteerit.

Kun tilat on luokiteltu, on suositeltavaa viestiä käyttäjille, mihin luokkaan yksittäinen tila kuuluu. Tilaluokan voi viestiä kyltein tai muunlaisin opastein, jotka sijoitetaan esimerkiksi vyöhykkeen rajalle. Tällöin on selvää, milloin siirrytään vyöhykkeeltä toiselle. Opasteiden lisäksi tulee luoda tilan käyttäjiä varten ohjeistus koskien sitä, millä kriteereillä missäkin tilaluokassa saa olla ja mitä tietoa siellä saa käsitellä. Näkyvä opaste kertoo yksiselitteisesti tilassa oleville, mihin käyttöön ja kenelle tila on tarkoitettu, mikä selkeyttää tilojen käyttöä. Näkyvä tilaluokitus antaa myös selkeän perusteen puuttua tilanteeseen, mikäli tilassa on henkilö, jolla ei ole oikeutta oleskella kyseisessä tilassa. Kaikkien nähtävillä olevat ohjeet tukevat turvallisuusohjeistuksen noudattamista; toisen henkilön kulkemiseen ja oleskeluun puuttuminen ei ole vain kahden henkilön välinen asia vaan osa organisaation toimintatapoja.

Tilojen luokituksen tekeminen näkyväksi voi teoriassa toimia tunkeutujaa auttavana tekijänä – tunkeutujan on helppo havaita tärkeä tila. Tässä kuitenkin korostuu aiempien suojakerrosten merkitys. Mikäli tiloissa liikkumista on rajoitettu, kulunhallinnan prosessit toimivat ja henkilökunta on valpasta ja toteuttaa vierailijakäytäntöä, jää riski tunkeutujan pääsemisestä sisään rakennukseen pieneksi. Näin ollen näkyvästä tilaluokittelusta on enemmän hyötyä kuin haittaa.

Tilojen luokittelu on pohjana myös kulunhallinnan määrittelyille; tilaluokittelun pohjalta voidaan luoda eri käyttäjäryhmille suunnatut kulkuoikeusryhmät. Tilaluokkien yhteyksiä erilaisiin kulkuoikeuksiin on havainnollistettu kuvassa 7. Esimerkiksi urakoitsijalle voidaan antaa kulkutunniste tai mekaaninen avain, jolla pääsee vain niihin tiloihin, joihin

hänellä on työtehtävänsä puolesta tarve päästä. Tapauksesta riippuen, kulkuoikeus voi kattaa puolijulkisen ja hallinnollisen alueen tai pelkästään hallinnollisen alueen. Kulunhallinnan ja pääsynhallinnan periaatteet on kuvattu tarkemmin liitteessä 4.



Kuva 7: Tilaluokkien yhteydet erilaisiin kulkuoikeuksiin

Käytössä on myös yhteiskäyttötiloja, joissa toimii useita eri osapuolia. Tällaisia ovat esimerkiksi kiinteistöt, joissa toimii useita vuokralaisia. Lisäksi vuokralaisorganisaatioilla voi olla toisistaan poikkeavia käytäntöjä kulunhallinnan suhteen. Siinä missä yhdessä vuokralaisorganisaatiossa on hyvin avoin kulunhallintapolitiikka, voidaan toisessa vuokralaisorganisaatiossa rajoittaa kulkemista voimakkaasti. Näissä tilanteissa on tärkeää sopia tilojen omistajan tai vuokranantajan kanssa ehdoista, joilla vuokralaisen tiloihin saavutaan. Tämä voi tarkoittaa esimerkiksi sitä, että kiinteistöhuolto tai muu kiinteistön tilaama palveluntuottaja ei saa tulla vuokralaistilaan omilla avaimillaan vaan hänen tulee sopia käynnistään aina ennakkoon vuokralaisorganisaation kanssa. Kriittisimpien tilojen osalta on huomioitava mahdolliset turvallisuusselvitysvaatimukset.

2.3.2 Tietojen ja järjestelmien oikeanlainen käyttö

Tiedon merkitys nyky-yhteiskunnassa on valtavan kriittinen. Tietovuodot voivat pahimmillaan aiheuttaa taloudellisia menetyksiä, mainehaittaa ja organisaation asiakkaiden luottamuksen menetyksen, joissain tapauksissa oikeudellisia seurauksia ja pahimmillaan liiketoiminnan keskeytymisen. Yhteiskunnalle kriittisiä palveluita tarjoavan organisaatioiden tietojen päätymisellä vääriin käsiin voi olla vaikutuksia jopa yhteiskunnan toimintaan.

Suuri osa tiedosta on sähköisessä muodossa, mutta edelleen käytössä ovat muut tallennusmuodot kuten paperi, liikkuva kuva sekä äänitallennus. Tietojen suojaamisen keinot ovat osin yhteneviä fyysisen omaisuuden suojaamisen kanssa.

Tietojen luokittelu

Tietoja voidaan luokitella samoin perustein kuin tiloja.

- tiedot, jotka voi tai pitää jakaa julkisesti. Julkiset tiedot voidaan edelleen jakaa
  - avoimesti kaikkien saatavilla oleviin tietoihin
  - tietoihin, joita jaetaan rajatusti

- tiedot, jotka on tarkoitettu ainoastaan organisaatioon kuuluville
- tiedot, jotka on tarkoitettu vain työtehtäviensä puolesta niitä välttämättä tarvitseville

Tietojen suojaaminen niiden kriittisyysluokittelun mukaan

Mitä kriittisempi tieto, sitä enemmän on kiinnitettävä huomiota suojaustoimiin ja siihen, keillä on oikeus päästä käsiksi tietoon. Tietoturvan perusperiaatteet ovat tiedon eheyden, luottamuksellisuuden ja saatavuuden varmistaminen. Tietojen kriittisyysluokittelun ja tietoturvan periaatteiden avulla voidaan määritellä, minkälainen tieto tulee rajata vain tietyille käyttäjille, millä perusteilla, miten he pääsevät tietoon käsiksi. On myös huomioitava, kenellä on oikeus muokata tietoa ja millä perusteella.

Fyysisen suojauksen osalta tämä tarkoittaa fyysisessä tallennusmuodossa olevan kaikkein kriittisimmän tiedon sijoittamista siten, että se on mahdollisimman monen suojauskehän sisällä. Käytännössä tämä voi tarkoittaa esimerkiksi säilytystä rakennuksen sisäosissa kulunvalvottujen ovien takana sijaitsevassa kassakaapissa, johon on pääsy vain muutamalla nimetyllä henkilöllä.

Teknisten järjestelmien osalta tämä tarkoittaa laitosten toiminnan kannalta kriittisimpien järjestelmien sekä niiden sisältämien ja niihin liittyvien tietojen tunnistamista. Tämän luokitellun jälkeen tulee tunnistaa, millä käyttäjäryhmillä tulee olla mihinkin tietoihin pääsy työtehtäviensä takia. Käyttäjäryhmille annetaan järjestelmään vain niin laajat käyttöoikeudet kuin on tarpeen, ei enempää. Lisäksi tulee määritellä järjestelmän ylläpitoon liittyvät roolit ja niiden vastuuhenkilöt.

Järjestelmään luotavien käyttäjätunnusten tulee olla henkilökohtaisia ja yhteiskäyttötunnuksia tulee välttää. Tämä helpottaa jäljitettävyyttä. Järjestelmän käyttäjiä tulee opastaa käyttäjätunnusten tietoturvalliseen hallintaan eli siihen, että käyttäjätunnuksia ja salasanoja tai PIN-koodia ei koskaan tule antaa toiselle henkilölle edes hetkellisesti. Salasana on säilytettävä huolellisesti ja sen tulee olla laadultaan sellainen, ettei ulkopuolisen ole mahdollista sitä helposti päätellä. Käyttäjätunnuksia ja salasanoja ei tule ikinä säilyttää näkyvillä. Salasanojen ja käyttäjätunnusten hallintaan suositellaan siihen soveltuvaa ja luotettavaa salasanasovellusta.

2.3.3 Avainhallinta

Avainhallinnalla tarkoitetaan kaikkien tietyn fyysisen kohteen lukostoon kuuluvien avainten hallinnointia. Lukosto koostuu yksittäisen kiinteistön kaikista lukoista, jotka kuuluvat tietyn lukitusjärjestelmän piiriin (tietyn tyyppisellä avaimella aukeavat lukot). Kiinteistöissä voi olla päälukitusjärjestelmän ohessa käytössä myös yksi tai useampi, kattavuudeltaan rajattu lukitusjärjestelmä (esim. tilat, joihin kuljetaan elektromekaanisella avaimella tai kulkutunnisteella). Keskeistä on, että lukitusjärjestelmiä voidaan toteuttaa monilla eri yhdistelmillä, mutta kaikkia avausvälineitä tulee hallinnoida.

Alle on koottu avainhallinnan keskeisimmät asiat.

- Ajantasainen tieto kaikkien lukostoon kuuluvien avainten sijainnista.
    - Avaimen tulee olla joko säilössä tai sen henkilön hallussa, jolle avain on luovutettu. Kulkeminen tulee estää sellaisilla avaimilla, joiden sijainti tai haltija ei ole tiedossa.
- Avainten turvallinen säilytys.
    - Avaimia on säilytettävä siten, etteivät asiattomat henkilöt pääse niihin käsiksi.

    - Avain ei saa olla selkeästi tunnistettavissa tiettyyn kiinteistöön kuuluvaksi.
    - Säilytettäviä avaimia ja saavat käsitellä vain vastuutetut henkilöt. Tämä koskee myös tietoa, joka yhdistää avainyksilöt tiettyihin kohteisiin.
    - Tilan, jossa avaimia säilytetään, tulee täyttää Finanssialan rakenteellisen murtosuojausohjeen vaatimukset
- Luovutuskriteerien määrittely.
    - Millä perusteilla ja kenelle eri avaintyyppejä luovutetaan.
    - Liittyykö erityiskulkuoikeuksien saamiseen erityisiä vaatimuksia (esim. koulutus, perehdytys tms.)
- Avaimen tulee aina olla liitettynä tiettyyn henkilöön.
    - Tämä tarkoittaa sitä, että avainta ei voi lainata yrityksen nimiin, vaan avaimen kuittaa vastaanotetuksi luonnollinen henkilö.
        - Avaimen luovutuksen ehtona tulee olla henkilöllisyyden ja lainausperusteen todistaminen (esim. virallinen henkilökortti ja työmääräyksen).
- On suositeltavaa kirjata avainten luovutuskuittauksiin aina tarkat tiedot lainaajasta (nimi, yritys, puhelinnumero, lainauspäivä).
    - Avaimet saattavat olla lainaajan hallussa jopa vuosia ja mikäli avainhallintaa hoitavat henkilöt ehtivät tänä aikana vaihtua, voi lainaajan selvittäminen olla hyvin haastavaa ja jopa mahdotonta pelkän nimen perusteella.
    - Tilanne on samanlainen, mikäli avain on vaihtanut omistajaa kädestä käteen pitkällä aikavälillä eikä vaihdoksia ole kirjattu avainhallintaan.
    - Molemmissa tilanteissa avainhallintaa hoitavalla on vain tieto alkuperäisestä haltijasta, jolloin avaimen nykyisen sijainnin selvittämiseen on hyvin vähän keinoja.
    - Avainhallinnan ajan tasalla pitämiseksi suositellaan, että kaikista avaimen haltijan vaihdoista jää aina kirjallinen jälki (esim. avain siirtyy organisaation sisällä työntekijältä toiselle).
- Avaimen luovuttajan (avainhallinnan ylläpitäjän) on hyvä ohjeistaa luovutustilanteessa avaimen oikea käyttö.
    - Avain on henkilökohtainen, eikä sitä tule luovuttaa muille edes hetkellisesti.
    - Avainta tulee säilyttää niin, etteivät asiattomat voi saada sitä haltuunsa.
    - Mikäli avain katoaa tai syntyy epäilys, että se on joutunut vääriin käsiin, tulee asiasta ilmoittaa välittömästi avaimen luovuttaneelle taholle.
- Lainaan luovutettujen avainten palautumisen seuranta.
    - Palautumatta jääneet avaimet on kyettävä havaitsemaan nopeasti, jotta niihin voidaan reagoida asianmukaisesti (esim. palautuspyyntö, mahdollinen avaimen deaktivointi tai uudelleensarjoitus).
    - Sanktiointi.
        - Sanktioiden määrittely ja niistä viestiminen lainaajille ennen avaimen luovutusta on keino edistää niiden palautumista laina-ajan päätteeksi.
        - Toinen keino on sitoa avainten palautus ehdoksi urakan viimeiselle maksuerälle.
- Selkeän kokonaiskuvan luomiseksi on suositeltavaa huomioida kaikki kiinteistössä käytössä olevat avausratkaisut avaimia koskevassa kirjanpidossa.
    - Käytännössä tämä tarkoittaa sitä, että avainhallintavastaava hallinnoi kaikkia kiinteistön avausratkaisuja (esim. mekaaninen lukitus, kulunvalvontatunnisteet, koodit ym.).
    - Mikäli keskittäminen ei ole mahdollista, on tärkeää sopia yhtenevät käytännöt kaikkien avausratkaisujen hallinnoijien kesken.

Kulun- ja pääsynhallintaan liittyen on mahdollista luoda luotettujen toimijoiden kategoria, johon kuuluville voidaan luovuttaa hieman tavanomaista enemmän vapauksia esimerkiksi kulkuoikeuksien suhteen. Mikäli tällainen kategoria päädytään luomaan, on keskeistä määritellä tarkasti kriteerit ja määritelmä sille, minkälaista toimijaa voidaan pitää luotettuna tahona ja miten luotetun tahon oikeudet poikkeavat tavanomaisesta. Luotettujen toimijoiden kategoria on erityisen hyödyllinen alaluvussa 2.3.4. käsiteltyjen yhteiskäyttölukkojen hallinnoinnissa.

2.3.4 Yhteiskäyttölukot ja kolmannet osapuolet

Yhteiskäyttölukoilla tarkoitetaan sellaisia tiloja, joihin useilla eri organisaatioilla on tarve päästä. On mahdollista, että tällaiset tilat sijaitsevat yksittäisen organisaation omistamalla tontilla, jolloin on ratkaistava, miten organisaation ulkopuoliset toimijat pääsevät kulkemaan yhteiskäyttötiloihin.

Kiinteistöjen teletilojen lukitusta koskevien yleisten vaatimusten perustan luovat Liikenne- ja viestintävirasto Traficomin kiinteistön sisäverkkoja ja teleurakointia koskeva määräys M65 sekä suositus 306/2019 S Kiinteistöjen laitetilojen lukituksesta. Perustuslain 10 §:n mukaan puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton, lukituksella siis osaltaan suojataan kiinteistöissä sijaitsevia tietoverkkoja ja -laitteita ja tätä kautta niissä kulkevaa tietoa. Lisäksi Energiateollisuuden Verkkopalveluehdot VPE 2024 linjaavat seuraavaa:

Kohta 4.14.

- Jos jakeluverkonhaltijan hallinnassa oleva sähkölaitteisto tai -laite on käyttäjän tiloissa tai alueella, käyttäjän on järjestettävä jakeluverkonhaltijalle sopijapuolten hyväksymällä tavalla korvauksetta viivytyksetön pääsy sähkölaitteiston tai -laitteen luo mm. huolto-, tarkistus-, vianselvitys- tai korjaustöitä varten vuorokaudenajasta riippumatta.

Kohta 6.3.

- Käyttäjän tulee korvauksetta sallia verkonhaltijan mittauksen ja mittaustietojen siirron kannalta tarpeellisten laitteistojen asentamisen tiloihinsa sekä niiden säilyttämisen, huoltamisen, luennan ja muut tarpeelliset toimenpiteet tiloissaan.

Rakennuksen omistaja vastaa yhteisten teletilojen (mm. talo-, ali-, ja kerrosjakamot) lukituksesta, valvonnasta ja tietoturvallisuudesta. Yhteiset laitetilat lukitaan yleensä samoin kuin talojakamo ja on suositeltavaa, että kaikki kiinteistön laitetiloihin tarvittavat avaimet olisivat keskitetysti saatavissa yhdeltä taholta. Mikäli talojakamon avaimella ei kuitenkaan voi avata kiinteistön muiden laitetilojen lukkoja, tulee talojakamossa olla tieto siitä, mistä tarvittava avain on saatavilla tai mistä pyytää avausta. Traficom suositteleekin, että talojakamo lukitaan teleyritysten yhteiseen sarjaan kuuluvalla lukolla.

KTL1E on vuonna 2015 käyttöön otettu valtakunnallinen teletilojen lukitusjärjestelmä, joka on kehitetty laajassa yhteistyössä alan toimijoiden ja viranomaisten kanssa. Järjestelmän tavoitteena on ollut luoda turvallinen ja yhtenäinen ratkaisu, joka mahdollistaa palveluntarjoajien ja asentajien esteettömän kulun kriittisiin teknisiin tiloihin kaikissa tilanteissa. Yhtenäinen, erillinen lukitusratkaisu vähentää riippuvuutta erillisistä avauspalveluista, joiden saatavuuteen tai saapumisaikaan voi liittyä viivettä. Tämän ansiosta korjaushenkilöstö pääsee vikatilanteissa nopeasti työskentelemään, mikä lyhentää mahdollisten katkoksien kestoa.

KTL1E-järjestelmä edellyttää erillistä liittymistä, ja se on suunnattu muun muassa telealan toimijoille sekä sähkö-, tele- ja antenniurakoitsijoille, energia-, kaukolämpö- ja

vesihuoltolaitoksille ja pelastustoimelle. Järjestelmän toimitus ja käyttöön liittyvä hallinnointi on keskitetty valtuutetuille toimijoille, jotka ovat virallisesti liittyneet KTL1E:n käyttäjäksi. Järjestelmän avainpalvelu on keskitetty suoraan valmistajalle.

Finanssialan määritelmä mukaan kiinteistön seinään upotettu avainsäilö (putkilukko), on tarkoitettu kohteen reittiavaimen säilyttämiseen. Avainsäilössä olevalla avaimella erilaiset palveluntarjoajat pääsevät sisään kiinteistöön ja siellä edelleen työkohteeseensa. Näin avainsäilössä olevalla reittiavaimella päästään talojakamon ovelle asti, joka avataan erillisellä avaimella. Tällaisella vaiheistuksella mahdollistetaan ulkopuolisten henkilön työperusteinen pääsy kiinteistöön ja samalla rajoitetaan sellaisen henkilön kulkemista, joka on saanut käsiinsä avainsäilön avaimen muttei talojakamon avainta. Jotta tämä suojausmekanismi toimisi, on tärkeää, että reittiavaimet eivät käy talojakamon oven lukkoon ja ettei avainsäilössä säilytetä avainta, jossa on laajat kulkuoikeudet.

Nykypäivänä elektromekaaniset lukitusjärjestelmät mahdollistavat myös avaimettoman kulkemisen. Tällöin kulkeminen tapahtuu esimerkiksi älypuhelinsovelluksella. Toisissa järjestelmissä taas on käytössä avainten virkistyspiste, jossa sidosryhmään kuuluva voi aktivoida tietyn kohteen avaimen pitkän käyttötauon jälkeen. Virkistyspiste on seinään kiinnitettävä laite, joka vaatii toimiakseen virtalähteen ja tietoliikenneyhteyden.

Yhteiskäyttöön osallistuvien kesken on suositeltavaa sopia yhteinen toimintamalli, jonka jalkautuksesta kukin osapuoli vastaa omissa organisaatioissaan. Mikäli alueella toimii vartioimisliike, tieto tulee välittää myös heille. Yhteiskäyttöön liittyvät asiat kannattaa huomioida jo sopimustasolla esimerkiksi uutta toimitilaa vuokrattaessa/rakennuttaessa.

Toimintamallissa kannattaa huomioida seuraavat seikat:

- Yhteiskäyttökohteiden ja kaikkien niitä käyttävien sidosryhmien tunnistaminen.
- Omistus- ja käyttösuhteiden selvitys (tontin omistus, vuokralaissuhteet ym.).
- Eri käyttäjäryhmien kulkutarpeiden selvitys.
- Miten eri osapuolten kulkeminen käytännössä mahdollistetaan.
    - Mitkä sidosryhmät saavat käyttää mitäkin yhteiskäyttöön liittyviä avaimia.
    - Mitkä ovat kriteerit yhteiskäyttöavainten haltuun saamiselle.
    - Mahdolliset alueelle saapumiseen liittyvät ilmoituskäytännöt.
    - Mahdolliset avaimen käyttöön liittyvät käytännöt.
- Nimetty taho, joka vastaa yhteiskäyttöön liittyvien avainten hallinnasta ja avainsäilössä olevan avaimen ajantasaisuudesta.
    - Lukituksen hankinta- ja ylläpitokustannukset ovat kiinteistön omistajan vastuulla.
    - Avainhallintaa voi kuitenkin suorittaa toinen taho.

2.3.5 Henkilöresurssien hallinta

Fyysinen turvallisuus syntyy teknisten järjestelmien ja niiden käyttäjien toiminnan yhteisvaikutuksena. Jokaisessa vesihuoltolaitoksessa on oma turvallisuuskulttuurinsa ja se voi olla tasoltaan matala, korkea tai jotain siltä väliltä. Turvallisuuskulttuurin tasoon sekä henkilöstön turvallisuusosaamisen ja turvallisuustietoisuuden tasoon on mahdollista vaikuttaa perehdytyksillä ja koulutuksilla sekä pitämällä näitä teemoja jatkuvasti esillä organisaation arjessa. Keskeistä kaiken turvallisuuden kehittämistyön kannalta on se, että työllä on organisaation ylimmän johdon tuki.

Sisäisillä resursseilla tarkoitetaan organisaation omaa henkilökuntaa. Eri kokoisilla laitoksilla on erilaisia resursseja: osassa kaikki työ tehdään oman henkilökunnan voimin, toisissa taas käytetään ulkoistettuja palveluja.

Ulkoisilla resursseilla tarkoitetaan esimerkiksi palveluntuottajia, joilta organisaatio ostaa palveluja (esim. siivous, vartiointi, etävalvonta). Tiettyjen toimintojen ulkoistaminen palveluntuottajalle vapauttaa organisaation henkilökunnan resursseja ydintyön hoitamiseen. Ulkoisten resurssien hyödyntämisessä erityisesti turvallisuuden viitekehyksessä on kuitenkin huomioitava muutamia asioita.
Henkilöihin liittyy tiettyjä riskejä, jotka tulee huomioida turvallisuussuunnitelmassa. Normaalitilanteen häiriöihin varautumiseen kannattaa panostaa, sillä poikkeustilanteisiin varautuminen perustuu tähän suunnitteluun.

Avainhenkilöriski
Avainhenkilöllä tarkoitetaan sellaista työntekijää, jolla on paljon syvällistä osaamista jostakin erityisaiheesta, erityistaitoja tai laajoja vastuualueita ja jonka lähteminen organisaatiosta joko määräajaksi tai pysyvästi vaikeuttaa merkittävästi organisaation toimintaa. Poissaolo voi johtua ennakoitavissa olevista loma-ajoista, mutta myös vaikeasti ennakoitavista syistä kuten sairastumiset, onnettomuudet ja äkillinen työpaikan vaihto.

Osaamisen puutteesta syntyvät riskit
Työntekijän osaamisen riittämättömyys voi johtaa tilanteeseen, jossa työntekijä tahattomasti tuottaa haittaa organisaation toiminnalle. Osaamisen puute turvallisuusasioissa voi mahdollistaa ulkopuolisen henkilön luvattoman pääsyn sisään organisaation tiloihin järjestelmiin ja/tai tietoihin. Tällaisia tahattomuudesta syntyviä riskejä on mahdollista pienentää rajaamalla järjestelmien käyttöoikeuksia ja kulkuoikeuksia eri tiloihin roolien ja vastuiden mukaan, panostamalla perehdytykseen työsuhteen alkaessa sekä lisäkoulutukseen sen aikana.

Järjestelmätoimittajiin liittyvät riskit
Järjestelmätoimittaja tai ulkoistettu pääkäyttäjä voi päästä käsiksi useiden eri kohteiden järjestelmiin. Tällaisilla henkilöillä on hyvin laaja näkymä sekä mahdollisuudet muokata hallinnoimaansa järjestelmää. Näin ollen taustojen varmistaminen ja palvelun sisältöä koskeva tarkka dokumentaatio sopimustasolla auttavat varmistamaan toiminnan jatkuvuutta.

Ulkopuoliset kolmannet tahot
Oman riskinsä muodostavat kohteessa käyvät vierailijat, urakoitsijat, siivoojat ym. Riski syntyy, kun henkilö päätyy (vahingossa tai tahallisesti) sellaiseen tilaan, jossa hän voi satuttaa itsensä tai vahingoittaa prosessia tai laitetta tai pääsee käsiksi suojattavaan tietoon. Tavoite on, että organisaatio tietää, keitä sen tiloissa liikkuu ja että tiloissa liikkuvien kulkua on rajoitettu työtehtäviin liittyvin perustein. Ulkopuolisiin ryhmiin kuuluvat myös sellaiset organisaation lähialueen toimijat, jotka voivat toiminnallaan tuottaa riskin pohjavesilähteen saastumiselle. Tähän liittyvää riskiä on mahdollistaa pienentää viestimällä oikeista toimintatavoista.

Insider-riski
Insider-riskillä tarkoitetaan tilannetta, jossa organisaatioon kuuluva henkilö toimii työnantajaansa vahingoittavalla tavalla. Toiminnan taustalla voi olla henkilökohtaista kaunaa tai ulkopuolisen taho vaikutusta (työntekijän kiristäminen, lahjonta).

Hallintakeinoja

Avainhenkilöriskiä voidaan hallita tunnistamalla, miten organisaation toiminnalle kriittisimmät vastuut ja osaaminen jakautuu esimerkiksi seuraavien kysymysten kautta:

- Kuka vastaa mistäkin turvallisuusjärjestelmästä tai hallinnoi tiettyä turvallisuuden osa-aluetta tai prosessia?
- Kenellä on pääsy kaikkein kriittisimpiin järjestelmiin ja tietoihin?
- Miten varmistetaan toiminnan jatkuminen sekä pääsy kriittisiin tietoihin ja tiloihin tilanteessa, jossa ensisijainen vastuuhenkilö on estynyt?
- Miten varmistetaan, että kriittisimpien järjestelmien osaaminen on jakautunut organisaatiossa useammalle henkilölle?

- **Taustojen selvitys**
  Yksi keino insider-riskien sekä ulkopuolisten tahojen muodostamien riskein vähentämiseen ja torjuntaan erityisesti kaikkein kriittisimmissä kohteissa ja tehtävissä ovat turvallisuusselvitykset.

- **Turvallisuusselvitykset**
  Turvallisuusselvityksiä säätelee turvallisuusselvityslaki (726/2014). Turvallisuusselvityksen keskeiset tavoitteet:
  - Estää Suomen turvallisuuden kannalta olennaisten tietojen päätyminen vääriin käsiin
  - Varmistaa henkilön tai yrityksen luotettavuus tehtävissä, joissa käsitellään salassa pidettävää tietoa tai päästään kriittisiin tiloihin
- Turvallisuusselvityksiä tehdään henkilöille ja yrityksille, jotka toimivat tehtävissä, joissa edellytetään erityistä luotettavuutta.
- Suojelupoliisi (Supo) vastaa turvallisuusselvitysten tekemisestä. Supon kotisivuilta löytyy aiheeseen liittyvää tietoa ja ohjeita.

Kriittisen infrastruktuurin toimijat (energia-, vesi-, liikenne-, tietoliikenne) on erikseen mainittu kohderyhmänä. Selvityksen tulos ei ole viranomaisen arvio henkilön sopivuudesta, vaan taustatietojen tarkistus. Lopullisen arvion henkilön sopivuudesta tehtävään tekee työnantaja.

Turvallisuusselvitys ei korvaa muita turvallisuusjärjestelyjä, vaan täydentää niitä. Siksi henkilöturvallisuusselvityksen laatimisen yleisenä edellytyksenä on, että hakija on rajoittanut teknisin ja muin toimenpitein pääsyä suojattaviin tietoihin huolehtinut toimitilojen ja tietojärjestelmien suojaamisesta sekä ryhtynyt muihin asianmukaisiin toimenpiteisiin tietoturvallisuuden sekä muiden turvallisuusjärjestelyjen toteuttamiseksi. Turvallisuusselvityksen teettäminen edellyttää kirjallista suostumusta selvityksen kohteelta ja sen tulosten käsittelyssä on kiinnitettävä erityistä huomiota luottamuksellisuuteen. Turvallisuusselvitykset ovat yleensä voimassa viisi (5) vuotta.

Turvallisuusselvitystyyppejä on kaksi:

1. **Henkilöturvallisuusselvitys**
   - Henkilöturvallisuusselvitys kohteena ovat yksittäiset henkilöt ja se voidaan laatia suppeana, perusmuotoisena tai laajana. Sen tarkoitus on varmistaa henkilön nuhteettomuus tai luotettavuus. Henkilöturvallisuusselvitystä voi hakea selvityksen kohteen työnantaja tai toimeksiannon antaja niistä henkilöistä, jotka toimeksiannossa työskentelevät.

2. **Yritysturvallisuusselvitys**
    - Yritysturvallisuusselvitystä käytetään erityisesti viranomaisen hankinnoissa, joten tässä yhteydessä sitä ei käsitellä laajemmin.

Suppea henkilöturvallisuusselvitys voidaan turvallisuusselvityslain 21 §:än mukaan laatia sellaisesta palvelussuhdetta tai toimeksiantotehtävää hoitavasta henkilöstä, joka:

- työskentelee sellaisessa yhdyskuntatekniseen huoltoon taikka elintarvike- tai lääkehuoltoon kuuluvassa tai näitä palvelevassa tehtävässä, jossa voi aiheuttaa vakavaa vaaraa yleisön terveydentilalle tai turvallisuudelle;
- Henkilöturvallisuusselvitys tehdään rekisteritietoja tarkistamalla sekä tarvittaessa selvityksen kohdetta haastattelemalla. Selvitys tuottaa tiedot:
    - kohteen yleisistä olosuhteista
    - ulkomailla oleskelusta
    - ulkomaansidonnaisuuksista
    - muista seikoista, joilla on erityistä merkitystä arvioitaessa hänen riippumattomuuttaan ja luotettavuuttaan muutoinkin selvityksen perustana olevan tehtävän kannalta.

Perusmuotoinen henkilöturvallisuusselvitys voidaan turvallisuusselvityslain 19 §:än mukaan laatia sellaisesta palvelussuhdetta tai toimeksiantotehtävää hoitavasta henkilöstä, joka:

- toimii tehtävissä, joissa voi vahingoittaa yhteiskunnan toimivuuden kannalta välttämättömän infrastruktuurin toimivuutta tai kriittisen tuotannon jatkumista taikka voi näissä tehtävissään saamiensa tietojen oikeudettomalla käytöllä merkittävällä tavalla vaarantaa valtion turvallisuutta tai edistää järjestäytynyttä rikollisuutta;
- voi tietojärjestelmän pääkäyttäjänä tai muut toimivaltuutensa huomioon ottaen vahingoittaa viranomaisten toiminnan tai yhteiskunnan perustoimintojen kannalta keskeisten tietojärjestelmien toimivuutta tai niiden tietoturvallisuutta;

Laaja henkilöturvallisuusselvitys voidaan turvallisuusselvityslain 20 §:n mukaan laatia vain henkilöstä, joka käsittelee ylimmän turvallisuusluokan asiakirjoja ja sellaisia tietoja, joiden paljastuminen voi aiheuttaa vahinkoa valtiollisella tasolla. Näin ollen se ei sovellu vesihuoltolaitosten käyttöön eikä sitä tässä yhteydessä käsitellä tarkemmin.

Vesihuollon toimialalla suppean tai perusmuotoisen henkilöturvallisuusselvityksen teettäminen voi tulla kysymykseen sellaisten henkilöiden osalta, joilla on työtehtäviensä hoitamisen takia pääsy laitoksen toiminnan kannalta kriittisimpiin tiloihin ja tietojärjestelmiin, joiden kautta voidaan haitata välttämättömän infrastruktuurin toimivuutta tai kriittisen tuotannon jatkumista, aiheuttaa vakavaa vaaraa yleisön terveydentilalle tai turvallisuudelle tietojärjestelmän pääkäyttäjänä tai muut toimivaltuutensa huomioon ottaen vahingoittaa yhteiskunnan perustoimintojen kannalta keskeisten tietojärjestelmien toimivuutta tai niiden tietoturvallisuutta

Turvallisuusperehdytys

Turvallisuusperehdytys kokoaa yhteen keskeiset perusasiat organisaatiosta, sen käyttämistä tiloista ja organisaation edellyttämistä toimintatavoista. Kattavalla perehdytyksellä heti työsuhteen alussa voidaan nopeuttaa uuden työntekijän sopeutumista organisaatioon ja asiaa kertaamalla pidempään talossa olleiden kanssa varmistetaan, että kaikilla on yhtäläinen tietämys siitä, minkälaisia toimintatapoja organisaatio edellyttää. Tiedonvälityksen lisäksi turvallisuusperehdytyksen avulla viestitään henkilöstölle turvallisuuskulttuurista:

- Miten organisaatio suhtautuu turvallisuuteen
- Miten turvallisuutta koskeva vastuu jakautuu organisaatiossa johdosta työntekijöihin

- Mikä on käytössä olevien turvallisuuteen liittyvien toimintatapojen merkitys.

Turvallisuusperehdytys voi sisältää esimerkiksi:

- Tiedon turvallisuudesta vastaavista henkilöistä
  - vastuualueet
  - yhteystiedot
  - toivotut yhteydenottotavat
- Yleistasoisen kuvauksen siitä, miten kulunhallinta on järjestetty organisaatiossa
  - mitkä tilat ovat sallittuja vierailijoille
  - mitkä tilat ovat koko henkilökunnan käytössä
  - mihin tiloihin kulkemista on rajoitettu ja minkälaisen prosessin kautta pääsyä haetaan
    - Ymmärrys siitä, miten kulunhallinnan kokonaisuus ja sen perusprosessit toimivat ja mikä on niiden tarkoitus, auttaa havaitsemaan mahdolliset poikkeamat.
- Työsuhteen eri vaiheisiin liittyvät toiminnot
  - Miten toimitaan työsuhteen alussa, sen aikana ja päättyessä?
    - Keneltä saa tarvittavat avaimet ja pääsyn eri järjestelmiin?
      - Miten avaimia ja käyttäjätunnuksia hallinnoidaan?
      - Miten toimitaan, jos avain katoaa tai on epäilys, että käyttäjätunnus ja salasana ovat päätyneet vääriin käsiin?
      - Miten ja kenelle avaimet palautetaan työsuhteen loppuessa?
  - Selkeitä ja konkreettisia ohjeita eri tilanteissa toimimiseen
    - miten organisaatioon tulevia vierailijoita tulee ohjata
    - miten toimia, jos kohtaa tuntemattoman henkilön organisaation tiloissa
  - Selkeitä ja konkreettisia ohjeita turvallisuushavainnoista ilmoittamiselle
    - minkälaiset havainnot tulee ilmoittaa turvallisuudesta vastaavalle
    - mitä kautta havainnot tulee ilmoittaa
    - havainnoista tulee ilmoittaa viipymättä

2.3.6 Dokumentaation hallinta

Fyysisen ja hallinnollisen turvallisuuden viitekehyksessä dokumentaatiolla tarkoitetaan:

- Hallinnolliseen turvallisuuteen liittyviä asiakirjoja, selvityksiä ja kuvauksia
  - Näitä ovat esimerkiksi
    - Kulunhallinnan politiikka
    - Fyysisen turvallisuuden kehityssuunnitelma
    - Riskienarvioinnin tulokset
    - Kehitystoimenpiteiden toteutumista koskeva kirjanpito
    - Turvallisuushavaintoja koskeva kirjanpito
- Erilaisten turvateknisten järjestelmien teknisten tietojen kuvauksia
  - Näitä ovat esimerkiksi
    - laitesijoituskuvat
    - järjestelmäkaaviot
    - järjestelmän laajuutta ja toimintaa koskevat kuvaukset.

Dokumentaatio siis todentaa organisaation turvallisuutta koskevat päätökset, linjaukset ja sovitut kehitystoimet ja mahdollistaa niihin palaamisen pitkänkin ajan jälkeen. Ajantasainen dokumentaatio on hyvä pohja turvallisuustyön kehittämiselle ja nopeuttaa esimerkiksi johtotasolle tuotettavien erilaisten raporttien ja kuvausten tuottamista.

Aktiivisesti ylläpidetty dokumentaatio
- parantaa tiedon löydettävyyttä
- nopeuttaa päätöksentekoa
- vähentää virheitä.

Teknisten järjestelmien osalta ajan tasalla oleva dokumentaatio helpottaa ja nopeuttaa uuden järjestelmän hankinnan suunnittelua sekä urakan toteutusta. Dokumentaation merkitys korostuu tilanteissa, joissa teknistä järjestelmää uusitaan. Mikäli dokumentaatiosta on huolehdittu koko järjestelmän elinkaaren ajan (mikä tyypillisesti on noin 10–15 vuotta), on jo hankintaa suunnitellessa käytettävissä kattavaa ja luotettavaa tietoa sen laajuudesta, kaapeloinneista, laitteista ynnä muusta. Tämä vähentää ylimääräisen selvittelytyön tarvetta hankinnan yhteydessä ja säästää aikaa sekä kustannuksia. Luvussa 5.6 on käsitelty tarkemmin teknisten järjestelmien elinkaarta.

Hankintavaiheessa dokumentaation avulla voidaan määritellä urakkaan osallistuvien tahojen selkeät roolit ja vastuut. Kun vastuujaot on dokumentoitu kirjalliseen muotoon, on ne helppoa tarkistaa urakan eri vaiheissa sekä urakan päätyttyä. Tämä vähentää epäselvyyksiä ja parantaa yhteistyötä eri toimijoiden välillä.

On suositeltavaa, että laitokset määrittävät asiakirjoille tietoturvaluokitukset huomioiden asiakirjojen luottamuksellisuuden tason. Tietoturvaluokitukset ohjaavat asiakirjojen käsittelyn tapaa. Käsiteltävät asiakirjat (sähköiset tai fyysiset) voidaan luokitella esimerkiksi kolmiportaisesti:
1. **Julkinen** *(kaikille avoin tieto)*
2. **Sisäinen** *(vain vesilaitoksen henkilöstön tietoon ja/tai rajoitetusti määritetyille sidosryhmille)*
3. **Rajoitettu / luottamuksellinen** *(rajoitetusti vesilaitoksen henkilöstön tietoon ja/tai määritetyille sidosryhmille, vain tiedonsaantiperusteisesti)*

Tietoturvalliseen toimintatapaan liittyviä käytänteitä on käsitelty mm. *Vesihuollon toimintavarmuuden ja kyberturvallisuuden parantamisen yhteishanke VESKY 2025* -materiaaleissa. Nämä sisältävät erilaisia dokumentteja, joiden tarkoitus on tukea laitoksia antamalla valmiit pohjat ja esimerkit hallintamallien ja politiikkojen luomiseen, missä on valmiiksi sisällettynä näiden kannalta oleelliset aiheet sekä esimerkit näiden toteutuksesta.

2.4 TURVALLISUUSTOIMIEN KEHITTÄMISESTÄ SAAVUTETTAVA HYÖTY

Turvallisuuden kehittäminen vaatii aikaa, rahallista panostusta ja henkilöresursseja. Tilanteessa, jossa resurssit ovat valmiiksi rajalliset voivat nämä panostukset tuntua ylimääräisiltä ja turvallisuuteen liittyvien käytäntöjen tiukentaminen arkista toimintaa haittaavana. Tällainen ajattelu voi korostua erityisesti, jos organisaatio ei ole kohdannut suurempia häiriötilanteita ja sen toiminta on jatkunut pitkään tasaisena. Se, että häiriöitä ei aiemmin ole ollut, ei takaa sitä, että niitä ei voisi jatkossa olla – varsinkin globaalin turvallisuustilanteen muuttuessa epävarmemmaksi.

Turvallisuuden kehittämisen hyödyt ilmenevät tyypillisesti epäsuorasti ja turvallisuuden merkitys havaitaan usein vasta, kun jotain on jo tapahtunut. Turvallisuuden kehittämistä kannattaakin tarkastella ennakoivasta, eteenpäin katsovasta näkökulmasta: oikein kohdistetut kehitystoimet auttavat ehkäisemään häiriötilanteiden syntyä ja edesauttavat toiminnan sujumista mahdollisesta häiriöstä huolimatta. Työntekijän kannalta tämä tarkoittaa työpaikan toimivuuden varmistamista ja siten vakautta.

Turvallisuustoimien kehittämisen näkyvin hyöty on organisaation fyysisten rakenteiden suojauksen vahvistaminen ulkoisia uhkia vastaan. Hyödyt ulottuvat kuitenkin laajemmalle organisaatioon: turvallisuustoimien kehittämisen muita hyötyjä ovat:

1. Strateginen suunnittelu ja resurssien kohdentaminen

Riskien- ja kriittisyydenarviointityön lopputuloksena laitoksen kehitystarpeet on kartoitettu ja priorisoitu ja tämän tiedon perusteella voidaan luoda kehittämissuunnitelma.

Kehityssuunnitelma antaa suuntaviivat ja aikaraamit, joiden mukaan edetä. Toiminnan suunnitelmallisuus ja ennakoitavuus lisääntyy, mikä puolestaan helpottaa resurssien kohdentamista ja investointien järkevää suunnittelua ja mitoittamista. Kriittisyysluokittelu antaa myös perusteita sille, miksi tiettyihin toimiin tai hankintoihin tulee panostaa.

Esimerkki: Kriittisempien kohteiden suojaus huomioidaan kuluvan vuoden budjetissa, prioriteeriltään pienempien kohteiden suojaus on jaettu myöhemmille vuosille.

Käsitys oman kohteen yleisestä sekä sen yksittäisten laitteiden tai prosessien kriittisyydestä sekä tarvittavista suojaustoimista ja -tasosta auttaa luomaan uusille hankinnoille kriteerit, mikä helpottaa markkinoilla tarjolla olevien ratkaisujen valintaa.

Esimerkki: Suojaustarpeiden tarkka määrittely auttaa rajaamaan markkinoilla tarjolla olevista palveluista itselle sopivimman, joka vastaa organisaation tarpeisiin eikä sisällä lisäominaisuuksia, joista ei välttämättä ole suurta käytännön hyötyä.

Kohteen tarpeisiin sovitetut teknologiset ratkaisut tehostavat parhaimmillaan toimintaa, kun automatiikka hoitaa osan ihmisen tehtävistä. On kuitenkin tärkeää muistaa, että tekniikka ei korvaa ihmisen panosta ja että turvallisuustekniikan lisääminen voi myös lisätä resurssitarpeita laitoksella.

2. Toiminnan jatkuvuuden varmistaminen

Henkilökunnan turvallisuusosaamisen ja reagointikyvyn vahvistaminen on erityisen tärkeää vesihuollossa, joka on yhteiskunnan toiminnan kannalta elintärkeän toiminto. Erilaisiin normaalitilanteen häiriöihin varautuminen vahvistaa organisaation resilienssiä ja toimii pohjana vakavampiin häiriöihin varautumiselle.

3. Alan toimijoiden välinen yhteistyö

Resurssien ollessa rajalliset on hyvä pohtia mahdollisuuksia yhdistää resursseja toisen alan toimijan kanssa. Lisäksi turvallisuusasioita koskevan keskustelun lisääminen alan toimijoiden välillä antaa mahdollisuuden jakaa eri laitoksilla kehitettyjä hyviä toimintamalleja ja saada ne alan muiden toimijoiden käyttöön. Yksittäiset toimijat puolestaan voivat jalkauttaa hyviä käytäntöjä omaan toimintaansa tiedotuksella ja sisällyttämällä ne turvallisuusperehdytykseensä.

3 RISKIENARVIOINTI JA RISKIENHALLINTA

3.1 RISKIEN ARVIOIMINEN

Turvallisuuden kehittäminen vesihuollon kriittisissä kohteissa perustuu aina laitoksen omaan riskienhallintaan ja riskienarviointiin. Jos arviointi puuttuu tai on vanhentunut, se on päivitettävä ennen toimenpiteitä. Riskienarviointi ei ole pelkkä muodollisuus, vaan se toimii perustana kaikille kehitystoimille ja auditointityökaluna, kun verrataan nykytilaa suosituksiin.

Riskienhallinnan toimenpiteillä poistetaan, pienennetään tai siirretään olemassa olevia riskejä siten, että niiden toteutumisen aiheuttama haitta on organisaation hyväksymällä tasolla. Riskienhallinnan tavoitteena on tukea organisaation johtamista, päätöksentekoa, henkilöstön koulutusta ja perehdytystä. Sen avulla johto saa kokonaiskuvan merkittävimmistä riskeistä ja voi sovittaa päätöksensä sekä riskienhallintatoimenpiteet riskinkantokyvyn ja riskinottohalun puitteisiin. Riskienhallinta ei ole irrallinen prosessi, vaan sen tulee olla kiinteä osa strategiaa ja johtamista.

Riskien arviointi on turvallisuussuunnittelun perusta: siinä tunnistetaan organisaatiota ja sen tavoitteita uhkaavat tapahtumat, arvioidaan niiden todennäköisyys sekä taloudelliset ja toiminnalliset vaikutukset. Arvioinnin tarkoituksena on varmistaa, että tavoitteiden saavuttamista vaarantavat tekijät otetaan riittävästi huomioon. Prosessin tulee olla tapauskohtainen ja järjestelmällinen, jotta huomioidaan toimintaympäristö ja organisaation erityistarpeet. Näin vältetään geneeriset ratkaisut ja varmistetaan kustannustehokas, vaikuttava turvallisuussuunnittelu ilman yli- tai alimitoitusta.

Osana *Vesihuollon toimintavarmuuden ja kyberturvallisuuden parantamisen yhteishanke VESKY 2025* -hanketta on tuotettu vesihuollon kyberturvallisuuden riskienhallinnan työkalu, jota on mahdollista soveltaa myös muussa riskienarvioinnissa.

3.2 ISO 31000 -VIITEKEHYS JA PERIAATTEET

ISO 31000:2018 on kansainvälinen, toimialariippumaton standardi, joka määrittelee yhtenäiset periaatteet, rakenteen ja prosessin riskienhallinnalle. Se ei määrää yksityiskohtaisia menetelmiä, vaan tarjoaa yleispätevän ja skaalautuvan viitekehyksen, jota laitokset voivat soveltaa omiin tarpeisiinsa. Standardi toimii hyvänä perustana, koska se luo yhteisen kielen riskienhallinnalle ja tukee jatkuvaa parantamista sekä päätöksenteon johdonmukaisuutta.

Mallin keskeiset vaiheet ovat:

- **Toimintaympäristön määrittely**: Ennen riskien tunnistamista on ymmärrettävä toimintaympäristö, organisaation tavoitteet ja sidosryhmät. Vesihuollon kohdalla tämä tarkoittaa esimerkiksi laitoksen kriittisyyden arviointia huoltovarmuuden näkökulmasta.
- **Riskien tunnistaminen**: Kartoitetaan *vaarat ja uhkat*. Vesihuollossa näitä voivat olla esimerkiksi vaaralliset aineet, rikosuhka, henkilövahingot, palovaara tai järjestelmien toiminnan keskeytyminen.
- **Riskien analysointi ja arviointi**: Jokaisen tunnistetun *vaaran tai uhkan riski* arvioidaan todennäköisyyden ja vaikutusten perusteella. Näin saadaan käsitys siitä, mitkä riskit ovat kriittisimpiä.
- **Riskien käsittely**: Kun riskit on arvioitu, määritellään toimenpiteet niiden hallitsemiseksi. Tämä voi tarkoittaa fyysisiä suojauksia, teknisiä ratkaisuja tai toimintatapojen muutoksia.

- **Seuranta ja tarkastelu**: Riskienhallinta ei ole kertaluonteinen prosessi. Tilannetta on seurattava ja arvioitava säännöllisesti, jotta muutoksiin voidaan reagoida.
- **Viestintä ja konsultointi**: Läpinäkyvyys ja sidosryhmien osallistaminen ovat keskeisiä. Riskienhallinta onnistuu parhaiten, kun tieto kulkee ja eri toimijat ovat mukana.
- **Dokumentointi ja raportointi:** Riskienhallinnan prosessi ja tulokset dokumentoidaan läpinäkyvästi. Raportointi tukee päätöksentekoa ja jatkuvaa parantamista.

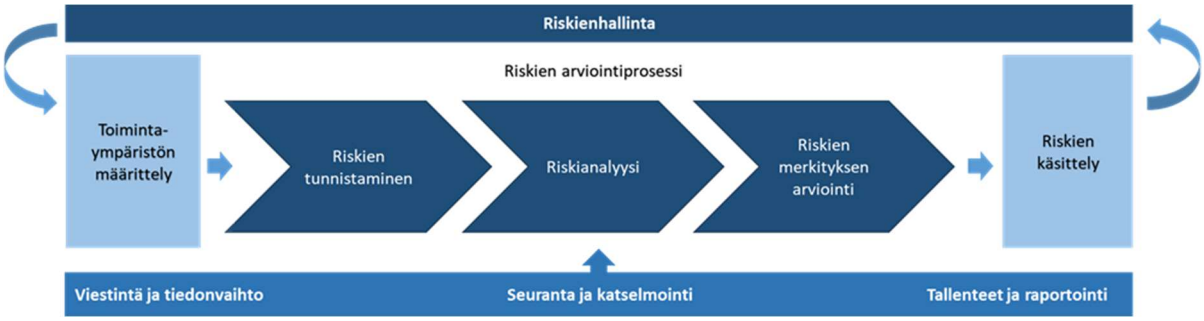
Näiden vaiheiden lisäksi ISO 31000 korostaa periaatteita, kuten integroitumista organisaation prosesseihin, systemaattisuutta, läpinäkyvyyttä ja jatkuvaa parantamista.

3.3 RISKIENHALLINTAPROSESSIN RAKENNE

Riskienhallintaprosessi perustuu organisaation sisäisten ja ulkoisten taustatietojen määrittelyyn, jotta saadaan kattava ymmärrys toimintaympäristöstä ja luodaan perusta oikein kohdennetulle riskienhallinnalle. Prosessin tarkoituksena on tunnistaa vesihuoltokohteen vaarat ja uhkat, analysoida niiden riskit ja päättää arvioinnin perusteella sopivimmat hallintakeinot. Riskienarviointi sisältää kolme päävaihetta: toimintaympäristön määrittämisen, riskien arvioimisen ja riskien käsittelyn. Näitä tukevat viestintä, yhteistyö, seuranta, katselmointi sekä dokumentointi ja raportointi.

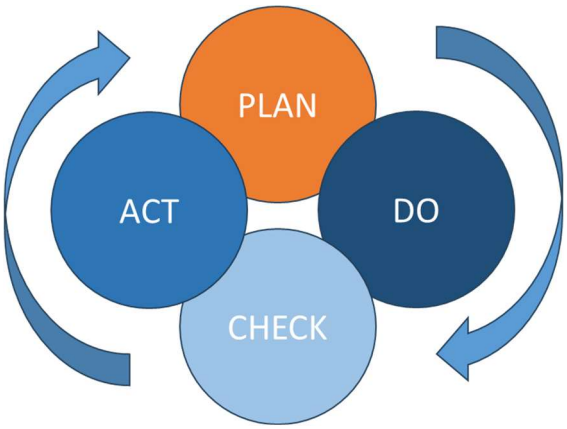
Riskienhallinta muodostuu kolmesta päävaiheesta:

1. **Toimintaympäristön määrittäminen:** Arvioidaan kohteen kriittisyys ja velvoitteet. Päätetään arvioinnin kattavuus (koko laitos vai yksittäinen kohde) ja riskinsietokriteerit.
2. **Riskien arvioiminen**: Tunnistetaan, analysoidaan ja arvioidaan riskien merkitys. Tämä vaihe jakautuu kolmeen osaan:
    a. Riskien tunnistaminen: Vaarat ja uhkat (esim. ilkivalta, tulipalo, toiminnan keskeytyminen, tietovuodot, elektroninen häirintä, avointen lähteiden tiedusteluun (Open Source Intelligece (OSINT) liittyvät uhat, sään ääri-ilmiöt).
    b. Riskien analysointi: Arvioidaan todennäköisyydet ja vaikutukset.
    c. Merkityksen arviointi: Priorisoidaan riskit kriittisyyden mukaan.
3. **Riskien käsittely**: Valitaan hallintakeinot:
    a. Riskin hyväksyminen
    b. Riskin siirtäminen (esim. vakuutus)
    c. Riskin poistaminen
    d. Todennäköisyyden pienentäminen
    e. Vaikutusten pienentäminen
    f. Riskirekisterien käyttö ja dokumentointi



Kuva 8 Riskienhallinta ja riskien arviointiprosessi

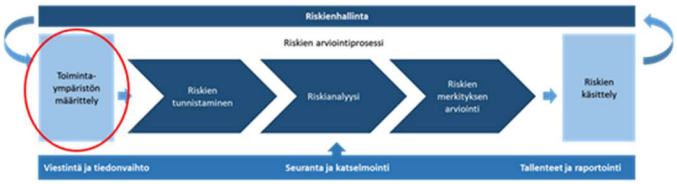
Tukiprosesseja ovat viestintä, yhteistyö, seuranta, raportointi ja tietosuojan varmistaminen. Riskienhallinta on jatkuva prosessi, jota kehitetään PDCA-mallin (Plan-Do-Check-Act) mukaisesti (kuva 9).



Kuva 9: PDCA-malli (Plan-Do-Check-Act)

3.3.1 Toimintaympäristön määrittäminen

Tässä prosessin vaiheessa luodaan perusta varsinaiselle riskien arvioimiselle (kuva 10). Tyypillisesti vaihe aloitetaan riskien arvioinnin kattavuuden määrittämisellä; arvioidaanko riskejä koko laitoksen tasolla vai kohdistetaanko se esimerkiksi yksittäiseen kohteeseen? Tätä seuraa riskien arvioinnin kriteerien määrittäminen, jossa arvioidaan sitä, kuinka paljon riskejä organisaatiossa ollaan valmiita sietämään / ottamaan.



Määritellään (=tunnistetaan ja rajataan):

- Mitä riskien arviointiin sisällytetään
- Sisäinen toimintaympäristö
- Ulkoinen toimintaympäristö
- Riskienhallintaprosessin toimintaympäristö kokonaisuudessaan
- Miten riskejä hallitaan

Rajaukset:

1. Keskitytään **normaaliolojen** turvallisuusriskeihin, jotka toteutuessaan **aiheuttavat vahinkoa organisaation toimitiloille, materiaaleille, tiedoille, tuotannolle, henkilöstölle tai organisaation maineelle.**
2. Juurisyinä **tarkoituksellisesti** (luvattomasti, pahantahtoisesti, tuottamuksellisesti) henkilöiden aiheuttamat teot tai tekoihin myötävaikuttaminen (=sisäiset ja ulkoiset Security riskit)
3. Keskitytään riskeihin, joiden todennäköisyyteen ja/tai vakavuuteen voidaan vaikuttaa **teknisillä ja/tai hallinnollisilla toimenpiteillä (=hallintatoimenpiteet).**

Kuva 10 Toimintaympäristön määrittäminen

- **Onko meillä riittävä ymmärrys toimintaympäristöstämme ja siihen vaikuttavista ulkoisista ja sisäisistä tekijöistä?**
- **Miten toimintaympäristön muutokset vaikuttavat riskeihimme?**
- **Mitä tietoa yrityksestämme on julkisesti saatavilla, tarvitaanko toimenpiteitä?**

3.3.2 Riskien arviointiprosessi

Riskien arviointivaiheessa tunnistetaan keskeiset riskit, analysoidaan niiden luonne ja arvioidaan merkityksellisyys (kuva 11). Tyypillisiä riskikategorioita ovat:

- Rikosriskit (Ilkivalta, varkaus tai ulkoinen vaikuttaminen)
- Onnettomuusriskit (Kuten tulva tai tulipalo)
- Keskeytysriskit (Kuten toiminnan keskeytyminen ja häiriöt)
- Henkilöriskit (Sisäiset sekä ulkoiset toimijat)
- Tietoriskit (Kuten salassa pidettävän tiedon vuotaminen)
- Open Source Intelligence (OSINT, tiedonkeruuta ja -analyysiä julkisista ja avoimista lähteistä)
- Sään ääri-ilmiöt ja luonnon katastrofit

Kolme vaihetta tiivistäen:
1. Tunnistetaan mitä negatiivista voi tapahtua
2. Analysoidaan em. Todennäköisyydet ja vaikuttavuudet
3. Saadaan riskiluku, jonka perusteella riskit voidaan järjestää ja priorisoida niiden merkittävyyden perusteella

Arviointiprosessin kulku:

1. **Riskien tunnistaminen**
   1. Tarkastellaan mahdollisia riskejä eri näkökulmista
   2. Yksilöidään riskit, eli ”ei toivotut” tapahtumat
2. **Riskianalyysi (riskimatriisilla)**
   1. Arvioidaan todennäköisyydet
   2. Arvioidaan vaikuttavuus
3. **Riskien merkityksen arviointi**
   1. Todetaan riskiluku (arviointityökalu)
   2. Arvioidaan merkitystä tarvittaessa tarkemmin

Kuva 11 Riskien arviointiprosessi

- **Mitkä ovat merkittävimmät riskit (esim. rikos-, onnettomuus-, keskeytys-, henkilö- ja tietoriskit)?**
- **Onko riskien tunnistaminen tehty kattavasti ja järjestelmällisesti – vai onko jotain jäänyt huomaamatta?**

3.3.3 Riskien käsittely

Riskien käsittelyssä valitaan sopivin tapa hallita tunnistettu riski analyysin ja merkityksen arvioinnin perusteella (kuva 12). Vaihtoehtoja ovat riskin hyväksyminen, siirtäminen (esim. vakuutus), poistaminen, todennäköisyyden pienentäminen, vaikutusten rajoittaminen sekä riskirekisterien käyttö.

Valinta tehdään aina tapauskohtaisesti, ja siihen vaikuttavat taloudellinen tilanne, tavoitteet, riskinsietokyky sekä muut erityistarpeet.

Kuva 12 Riskien käsittely

- **Mitä vaihtoehtoja meillä on riskien käsittelyyn (hyväksyminen, siirtäminen, poistaminen, pienentäminen)?**
- **Onko valitut riskienhallintatoimenpiteet suhteutettu riskinsietokykyyn ja tavoitteisiin?**
- **Miten varmistamme, että toimenpiteet ovat kustannustehokkaita ja vaikuttavia?**

3.3.4 Käytännön arviointiprosessi vesihuollossa

Käytössä olevat WSP / SSP tukevat pääasiassa laitoksen yleistä riskienarviointia. Niitä on suositeltava käyttää, koska ne on kehitetty nimenomaisesti vesihuollon tarpeisiin, mutta niillä ei ole mahdollisuutta saada kattavaa näkemystä fyysiseen turvallisuuteen kohdistuvista uhkista. Tässä oppaassa esitetty riskienarviointimallia voidaan käyttää arvioitaessa fyysisen turvallisuuden riskejä ja uhkia laitostoimintaan, eli se syventää tämän oppaan sisällön mukaisesti tarkastelua.

Varmuusluokitusohje vesihuoltolaitoksille auttaa arvioimaan kohteen kriittisyyttä. WSP- ja SSP-menetelmät tukevat vesihuollon riskienarviointia kokonaisvaltaisesti:

1. **Varmuusluokitusohje vesihuoltolaitoksille**
   a. Tarkoitus: Arvioi vesihuoltolaitoksen kriittisyyttä huoltovarmuuden näkökulmasta.
      i. Varmuusluokituksessa tarkastelu tehdään <u>vedenjakelualueittain</u> tilanteessa, jossa vedenjakelualueen pääasiallista vesilähdettä ei voida käyttää jonkin äkillisen syyn vuoksi useampaan vuorokauteen. Varmuusluokituksen tavoitteena on kuvata laitoksen keskimääräistä kykyä toimittaa vettä talousvesiverkostoon liittyneille asukkaille ja yhdyskunnan kannalta kriittisille toiminnoille tällaisessa tilanteessa.
   b. Käyttö: Luokittelun avulla tunnistetaan laitokset ja kohteet, joiden toiminnan häiriö aiheuttaisi merkittävän vaikutuksen yhteiskunnan toimivuuteen. Tämä tukee priorisointia, kun päätetään mihin kohteisiin kohdistetaan suojaustoimenpiteitä.
      i. Sen avulla kunnat ja vesihuoltolaitokset pystyvät arvioimaan kykyään selviytyä vedenhankintaan vaikuttavissa häiriötilanteissa.
   c. Hyöty: Auttaa muodostamaan kokonaiskuvan laitoksen merkityksestä ja ohjaa resurssien kohdentamista.
      i. Varmuusluokitustieto tukee ensisijaisesti <u>vesihuoltolaitosta</u> mm. vesihuoltolain mukaisen varautumissuunnitelman ylläpitämisessä

sekä näihin liittyvässä varavedenjakelun suunnittelussa ja pitkäjänteisessä investointisuunnittelussa.

ii. Kunta pystyy hyödyntämään alueensa vesihuoltolaitosten vedenjakelualueiden varmuusluokitustietoa vesihuoltolain velvoittamaan vesihuollon kehittämissuunnittelun sekä valmiussuunnittelun tukena.

iii. ELY-keskus käyttää varmuusluokitusta vesihuollon alueellisessa kehittämisessä. ELY-keskus toimittaa varmuusluokituksesta yhteenvedon Maa- ja metsätalousministeriölle.

Huom! ELY-keskusten toiminta päättyi vuoden 2025 lopussa ja uudet elinvoimakeskukset aloittivat toimintansa 1.1.2026. Suurin osa ELY-keskusten tehtävistä siirtyy elinvoimakeskuksille.

2. WSP (Water Safety Plan)

a. Tarkoitus: Talousveden riskinhallintajärjestelmä, joka perustuu WHO:n suosituksiin ja STM:n ohjeisiin.
b. Sisältö: Kattaa koko vedentuotantoketjun riskit – raakaveden otosta jakeluun. Tunnistaa uhkia, arvioi riskejä ja määrittää hallintakeinoja veden laadun turvaamiseksi.
c. Hyöty: Varmistaa, että vesihuoltolaitos täyttää lainsäädännön vaatimukset ja pystyy hallitsemaan riskejä järjestelmällisesti.

3. SSP (Sanitation Safety Plan)

a. Tarkoitus: Yhdyskuntajätevesihuollon riskinhallintajärjestelmä, STM:n ohjeistuksen mukainen.
b. Sisältö: Keskittyy jätevesihuollon prosesseihin ja niihin liittyviin riskeihin, kuten ympäristö- ja terveysvaikutuksiin.
c. Hyöty: Tukee turvallisuussuunnittelua ja varmistaa, että jätevesihuolto toimii häiriöttömästi ja turvallisesti.

Nämä riskienarviointimallit ottavat kantaa rajatusti fyysisen turvallisuuden uhkiin ja riskeihin, joten arviointia tulee laajentaa alla olevan prosessin mukaisesti.

1. Varmuusluokitusohje vesihuoltolaitoksille voi antaa lisätietoa laitoksen kriittisyysarvioinnin määrittämiseen.

2. Fyysisen turvallisuuden toteuttaminen ja sitä tukeva ”jatkoprosessi”:
   a. Riskienarviointi hyödyntäen perinteistä prosessia (fyysiset uhat) kuten kuvattu kappaleessa *3.3 RISKIENHALLINTAPROSESSIN RAKENNE*
   b. Fyysisen turvallisuuden suositustyökalun hyödyntäminen (kriittisyysluokittelu & suositukset, liite 6)
   c. Fyysisen turvallisuuden suojauskeinojen määrittäminen laitokselle ja sen kohteisiin perustuen riskienarviointiin ja toiminnan kriittisyysarviointiin.

4 FYYSINEN TURVALLISUUS

4.1 FYYSISEN TURVALLISUUDEN PERUSTEET

Tässä oppaassa fyysisen turvallisuuden suojaamisen keinot on jaettu kolmeen eri kategoriaan:

1. **Rakenteellinen suojaus**
   - Fyysiset rakenteet, erilaiset tilatyypit kriittisyyden mukaisesti, muut rakenteellista suojausta tukevat arkkitehtuuriset-, ympäristö- tai tekniset ratkaisut
2. **Tekninen suojaus**
   - Valvonta- ja hälytysjärjestelmät
3. **Operatiivinen suojaus**
   - Sisäiset ja ulkoiset resurssit, prosessit ja ohjeistukset, harjoitukset ja koulutukset, huolto ja ylläpito, jatkuvuuden varmistaminen

Erilaisilla fyysisen suojauksen keinoilla on erilaisia ominaisuuksia. Ne perustuvat erilaisiin keinoihin vaikuttaa tai hallita esimerkiksi oikeudetonta kulkua vesihuoltokohteeseen.

Tätä opasta ja siihen liittyvää työkalua (liite 6) käyttäessä on tärkeää huomioida se, että opas ja työkalut tuottavat suosituksia erilaisista suojausratkaisuista. Tämä tarkoittaa sitä, että jokaisen laitoksen tulee aina arvioida omat riskinsä ja tämän jälkeen arvioida riskiperusteisesti omaan tilanteeseensa soveltuvia suojausratkaisuja.

Esimerkki: Työkalu (liite 6) voi suositella tietyn tyyppiselle kohteelle suojausratkaisuksi aitaa, mutta työkalua käyttävällä laitoksella ei ole realistista mahdollisuutta toteuttaa tätä. Laitoksen tulee tällaisessa tilanteessa arvioida, minkälaisella muulla ratkaisulla voidaan lisätä turvallisuutta (esim. tilojen vyöhykkeistäminen, turvateknisiin järjestelmiin panostaminen tms.).

Tässä oppaassa keinojen ominaisuudet ovat jaettu kuuteen eri kategoriaan:

1. Ennaltaehkäistä, estovaikutus (Deter)
Tavoitteena on vähentää matalan tason hyökkäysten todennäköisyyttä. Tämä ei pysäytä hyökkäystä, mutta luo vaikutelman valvonnasta ja vaikeasta pääsystä.
Esimerkkejä: aidat, portit, valaistus, opasteet, näkyvä valvontalaitteisto.

2. Havaita (Detect)
Tarkoitus on tunnistaa, kun joku ylittää valvontalinjan. Havaitseminen ei estä hyökkäystä, mutta antaa varhaisen varoituksen.
Esimerkkejä: ovikoskettimet, liiketunnistimet, virtuaaliset hälytysrajat, kamerat ja tutkat.

3. Tarkkailla / tunnistaa (Observe)
Mahdollistaa jatkuvan visuaalisen seurannan ja tilanteen arvioinnin. Havainnointi tukee reagointia ja tilannekuvan ylläpitoa.
Esimerkkejä: kamerat (valvontakamerat ja lämpökamerat), tutkajärjestelmät, automaattinen tallennus ja etäkatselu.

4. Hidastaa (Delay)
Pidentää aikaa, joka hyökkääjältä kuluu etenemiseen. Viivytys antaa lisäaikaa reagointiin ja voi estää kriittisen kohteen murtamisen. *Esimerkkejä: rakenteellinen suojaus, vahvennetut rakenteet, ajoneuvoesteet /-hidasteet, henkilöstö.*

5. Evätä (Deny)
Rajoittaa pääsyn/kulkemisen vain valtuutetuille käyttäjille. Estämisen tehokkuus riippuu pääsyn- tai kulunhallinnan laadusta.
Esimerkkejä: kaksivaiheinen tai monivaiheinen tunnistautuminen, tilojen kriittisyysluokittelu ja siihen perustuva pääsynhallinta, lukitus, henkilökohtaiset kulkutunnisteet ja pääsyoikeudet.

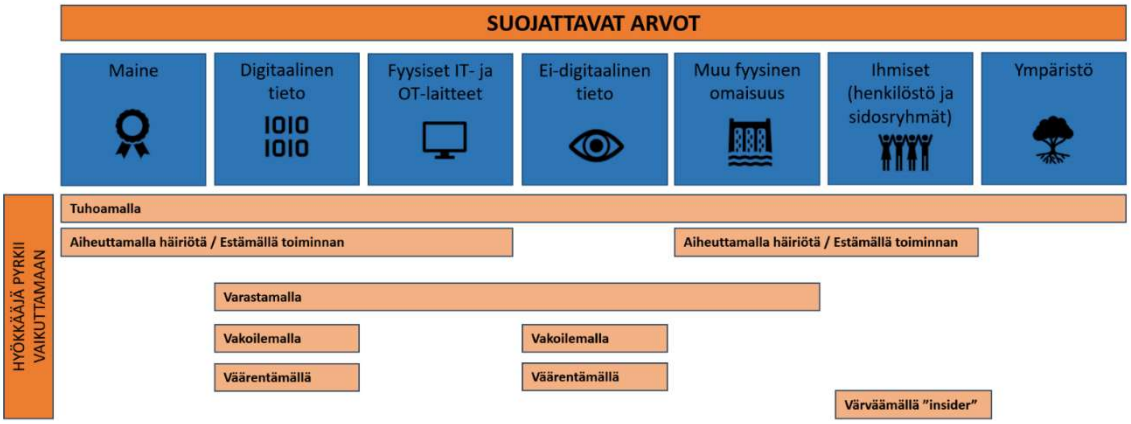
6. Reagoida (Respond)
Sisältää suunnitellut toimenpiteet hyökkäyksen varalta. Reagointi edellyttää ohjeita ja viestintää, jotta tilanne hallitaan nopeasti.
Esimerkkejä: hälytykset, vilkkuvalot, kaksisuuntainen ääniyhteys, ilmoitukset viranomaisille, toimintaohjeet sisäisille ja ulkoisille resursseille (esim. oma henkilöstö, vartioimisliike).

	Estää	Havaita	Tarkkailla / Tunnistaa	Hidastaa	Evätä	Reagoida
Kameravalvontajärjestelmä	X	✓	✓	X	X	✓
Kulunvalvontajärjestelmä	✓	✓	X	X	✓	X
Rikosilmoitinjärjestelmä	X	✓	✓	X	X	✓
Rakenteellinen suojaus	✓	X	X	✓	✓	X
Lukitustekniikka	✓	X	X	✓	✓	X
Vartiointipalvelut	✓	✓	✓	X	X	✓

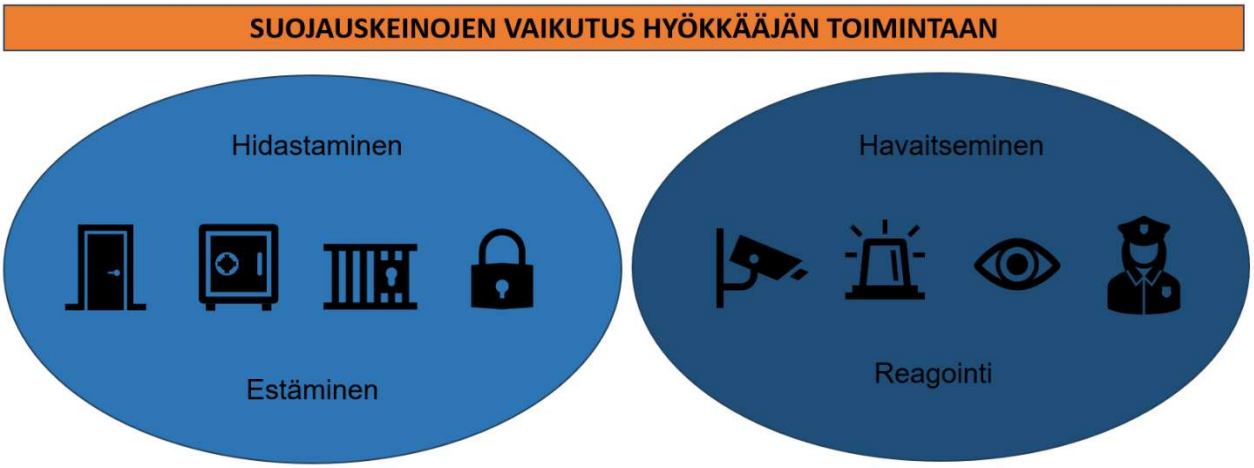
Kuva 13: Fyysisen turvallisuuden keinovalikoima ja niiden ominaisuudet

Suojattavat arvot

Suojattavilla arvoilla tarkoitetaan organisaatiolle tärkeitä asioita, joiden suojaaminen on sille tärkeää. Tyypilliset suojattavat arvot ja niihin kohdistuvat uhat esitetään kuvassa 14. Näitä arvoja suojataan erilaisilla fyysisen suojauksen keinoilla, joilla pyritään hidastamaan ja estämään luvatonta tunkeutumista rakennuksiin ja rakennelmiin sekä havaitsemaan alkava tai käynnissä oleva tunkeutuminen ja reagoimaan siihen (kuva 15).



Kuva 14: Tyypilliset suojattavat arvot ja niihin kohdistuvat uhkat



Kuva 15: Teknisten ja rakenteellisten ratkaisujen sekä vartioinnin käyttötarkoitukset fyysisessä suojautumisessa

Vesihuoltolaitokseen ja sen eri kohteisiin valittavat suojauskeinot tulee perustua riskienarviointiin. Tämän avulla voidaan määrittää, mitkä kohteet suojataan ja missä laajuudessa sekä määrittää toteutuksen tärkeysjärjestys. Oppaan kohdassa 3.3 on kuvattu riskienhallinnan ja riskienarvioinnin perusteet sekä kohdassa 4.3 kuvattu kohteen kriittisyyden arviointiin vaikuttavia tekijöitä.

Miten parantaa turvallisuutta rajallisilla resursseilla?

Jos vesihuoltolaitoksen talous- ja henkilöstöresurssit ovat rajalliset, voidaan turvallisuuden parantaminen aloittaa esimerkiksi seuraavista kustannustehokkaista vaihtoehdoista:

Toimenpide	Tavoite	Toteutustapa	Kategoria
Turvallisuus-kulttuurin kehittäminen	Parantaa osaamista ja käytäntöjä, nopeuttaa reagointia poikkeus-tilanteissa	*Koulutus, ohjeistus ja perehdytys *Osana työarkea	• Operatiivinen suojaus
Avainhallinnan selvitys	Estää luvaton pääsy	*Nykytilaselvitys, *Lukkojen päivitys kriittisiin tiloihin, jos epäselvyyttä avain-hallinnassa	• Operatiivinen suojaus • Rakenteellinen suojaus
Valaistuksen parantaminen	Lisää turvallisuutta ja ennaltaehkäisevää- / estovaikutusta	*Valaistuksen laajentaminen tai valaisintyyppien vaihtaminen	• Rakenteellinen suojaus
Yksinkertaiset hälytysratkaisut	Antaa varoituksen ja välittää tietoa	*Kuorivalvonta murtoilmaisujärjestelmällä tai IoT-sensoreilla	• Tekninen suojaus
Lukituksen parantaminen	Estää luvaton pääsy kriittisiin tiloihin	*Lisää riippulukkoja tai turvalukkoja.	• Rakenteellinen suojaus
Poikkeamien seuranta	Parantaa reagointia ja oppimista.	*Yksinkertainen poikkeamailmoituslomake (paperi tai sähköinen).	• Operatiivinen suojaus
Selkeät opasteet ja varoitusmerkinnät	Ohjata liikkumista ja vähentää tahattomat pääsyt rajoitetuille alueille.	*Hyödynnä näkyviä opasteita ja varoituskylttejä	• Hallinnollinen suojaus

Taulukko 1: Turvallisuuden parantamisen kustannustehokkaat vaihtoehdot

4.2 FYYSISEN TURVALLISUUDEN KOKONAISUUS JA RIIPPUVUUSSUHTEET

Fyysinen turvallisuus muodostuu kolmesta toisiaan tukevasta osa-alueesta. Kokonaisuus on kolmiosainen rakenne: jos yksi osa pettää, koko fyysisen turvallisuuden vakaus heikkenee merkittävästi.

Kaikkea fyysiseen turvallisuuteen liittyvää toimintaa ei voi eikä pidä ulkoistaa. Riittävä oma osaaminen ja vastuuhenkilöt tulee säilyttää vesihuoltolaitoksella, jotta toimintavarmuus ja turvallisuus voidaan taata myös muuttuvissa olosuhteissa ja poikkeustilanteissa. Näin varmistetaan, että vesihuoltolaitoksella on kyky hyödyntää tietoa ja reagoida nopeasti mahdollisiin uhkiin tai poikkeamiin. Turvallisuuskulttuurin kehittäminen tukee myös tätä tavoitetta.

Kuva 16: Esimerkkikuvaus eri toimintojen riippuvuussuhteista ja vaikutuksesta fyysisen turvallisuuden toteutumiseen

Kehäsuojausmalli
Tämä kategoria kattaa fyysiset ja tekniset elementit, kuten rakenteellinen turvallisuus (aidat, lukitukset, rakenteet), tekniset turvajärjestelmät (valvonta- ja hälytysjärjestelmät) sekä jatkuvuuden varmistaminen (mm. varavoima). Kehäsuojaus luo konkreettisen esteen ja valvontakerroksen, joka suojaa kriittisiä kohteita. Se on näkyvin osa fyysistä turvallisuutta, mutta sen tehokkuus riippuu siitä, miten organisaatio hallinnoi käyttöä ja reagointia.

Organisaation toimintatavat ja hallinnollinen turvallisuus
Tähän kuuluvat henkilöstön osaaminen, prosessit ja ylläpito. Tekninen suojaus ei ole riittävä ilman selkeitä toimintamalleja, kuten kulkuoikeuksien hallintaa, häiriötilanteiden

ohjeistuksia ja säännöllisiä tarkastuksia. Hallinnollinen turvallisuus varmistaa, että tekniset ratkaisut toimivat oikein, vesihuoltolaitoksen henkilöstö osaa käyttää niitä sekä poikkeamista ilmoitetaan ennalta sovittujen käytäntöjen mukaisesti. Hallinnollinen turvallisuus myös luo kulttuurin, jossa turvallisuus on osa jokapäiväistä toimintaa.

Kolmannet osapuolet
Palveluntuottajat, viranomaiset ja muut sidosryhmät muodostavat ulkoisen verkoston, joka tukee organisaation omaa turvallisuutta. Esimerkiksi vartiointipalvelut, huoltoyhtiöt ja viranomaisyhteistyö ovat kriittisiä häiriötilanteiden hallinnassa. Sopimukset ja vastuunjaot varmistavat, että ulkopuoliset toimijat noudattavat samoja turvallisuusstandardeja.

Kehäsuojausmalli on perusta, mutta ilman hallinnollisia käytäntöjä se jää passiiviseksi. Esimerkiksi kameravalvonta ei auta, jos hälytyksiin ei reagoida.
Organisaation toimintatavat ohjaavat teknisten ratkaisujen käyttöä ja varmistavat, että kolmansien osapuolten toiminta on linjassa organisaation tavoitteiden kanssa.
Kolmannet osapuolet täydentävät organisaation kyvykkyyksiä, mutta niiden hallinta edellyttää selkeitä prosesseja ja sopimuksia.

4.3 KRIITTISYYDEN ARVIOINTI

Moniosaisessa vesihuoltokohteessa, jossa on useita toimintoja ja omaisuuseriä (esim. vedenkäsittely, pumppaamot, varastot ja ohjausjärjestelmät), kokonaiskriittisyys voi olla korkea. Yksittäiset tilat tai komponentit voivat kuitenkin saada toisistaan poikkeavia kriittisyysluokituksia niiden merkityksen perusteella. Tällaisissa tilanteissa on käytännöllisempää kohdentaa suojaustoimenpiteet sellaisiin vesihuoltokohteisiin, jotka tunnistetaan sisältävän kriittisiä omaisuuseriä – kuten ohjausjärjestelmiä, vedenkäsittelylaitteita tai varavoimajärjestelmiä – kuin käsitellä vesihuoltolaitosta ja sen kohteita yhtenä saman kriittisyysluokan kokonaisuutena.

Oppaan tueksi on luotu työkalu (liite 6), jonka tavoitteena on tukea vesihuoltolaitoksen fyysisen turvallisuuden kehittämistä. Työkalun avulla on mahdollisuus määrittää arvioitavan kohteen kriittisyys toiminnalle ja tämän perusteella työkalu antaa soveltuvia fyysiseen turvallisuuteen liittyviä suojauskeinojen suosituksia. Työkalu auttaa arvioimaan nykytilaa suhteessa suosituksiin ja sen avulla vesihuoltolaitos voi määrittää tarvittavat toimenpiteet ja vastuutahot fyysisen turvallisuuden kehittämisestä arvioitavaan kohteeseen.

Kohteen ja sen tilojen kriittisyys sekä suojaustarpeet

- Arvioi kohteen kriittisyys ja sen jälkeen sen eri tilojen kriittisyys turvallisuuden ja toiminnan jatkuvuuden näkökulmasta. Kriittisyys vaihtelee kohteittain ja vaikuttaa suoraan tarpeelliseen suojaustasoon. Arvioitavaksi mm. seuraavat tekijät:
    - kohteen käyttötarkoitus
    - siellä harjoitettava toiminta ja keskeytyksen vaikutukset
    - tiloissa säilytettävät laitteet, järjestelmät, omaisuus ja tietoaineisto
- Määritä kriittisimmille tiloille korkeampi suojaustaso. Vähemmän kriittisille tiloille riittää matalampi suojaustaso.
- Kriittisyyden arvioinnissa tulee huomioida monet tekijät, kuten:
    - toiminnon toimimattomuuden vaikutukset palveluun,
    - lainsäädännön ja sopimusten vaatimukset,
    - keskeytyksen pituus,
    - taloudelliset menetykset,
    - maine jne.

Hyödyt

- Suojaus mitoitetaan oikein suhteessa kohteen ja sen tilojen kriittisyyteen.
- Ratkaisut ovat tarkoituksenmukaisia ja kustannustehokkaita.
- Vältetään ylimitoitettu suojaus, joka nostaa kustannuksia ja vaatii mahdollisesti enemmän resursseja ylläpitoon.

Työkalussa käytettyjä vesihuoltokohteen kriittisyyteen vaikuttavia tekijöitä ja väittämiä arvioinnin tueksi:

- Palveleeko kohde kriittisiä asiakkaita tai kohteita (yhtä tai useampaa)? (Esim. sairaalat, elintarviketeollisuus, huoltovarmuuskriittiset toimijat jne.)
- Onko kohteen kautta mahdollisuus vaikuttaa talousveden laatuun ja/tai toimitukseen TAI viemäröinnin ja jätevedenpuhdistuksen vaatimustenmukaiseen käsittelyyn? (Terveysturvallisuus)
- Ylittääkö kohteessa tapahtuvan häiriön vaikutus 50 % laitoksen palvelemasta väestöstä?
- Aiheuttaako kohteen häiriö vakavia seurauksia alle 12 tunnissa?
- Onko kohteessa kriittisiä tietojärjestelmiä tai laitteita, jotka lamaannuttamalla tarkasteltavan kohteen toiminta voi keskeytyä?
- Onko kohteen toiminta-alueella merkittävä teollinen tai taloudellinen riippuvuus vesihuollosta?
- Viekö kohteen korvaaminen yli 48 h?
- Voiko kohteen mahdollisella häiriöllä tai sabotoinnilla vaikuttaa ympäristöturvallisuuteen?

Vesihuoltokohteiden kriittisyysluokittelu on jaoteltu kolmiportaisesti:

- Varmistettava, jos mahdollista
- Varmistettava aina
- Varmistettava korkealla tasolla aina

Varmistettava, jos mahdollista

- Sisältää perustoimintoja, mutta ei kriittisiä toimintoja, esim. tila on tukitoiminto, jonka keskeytys ei vaikuta olennaisesti ydintoimintaan
- On olemassa vaihtoehtoinen / korvaava järjestely, tai voidaan luopua toiminnasta pitkäaikaisestikin ilman merkittävää haittaa

Sisältää kaiken sellaisen toiminnan, jonka häiriintyminen tai uhkatilanteet vaarantavat toimintaa, taloutta, asiakassuhteita, terveyttä tai ympäristöturvallisuutta ***vähän tai ei ollenkaan*** *.*

Varmistettava aina

- Toiminnalle kriittistä tai melko kriittistä, esim. tilan toiminta on tärkeää, mutta mahdollista keskeyttää lyhytaikaisesti ilman suurta haittaa tai tilan toiminnan pysäytys aiheuttaa vain rajallisen vaikutuksen tuotantoon tai palveluun
- On olemassa vaihtoehtoinen / korvaava järjestely

Sisältää kaiken sellaisen toiminnan jonka häiriintyminen tai uhkatilanteet vaarantavat toimintaa, taloutta, asiakassuhteita, terveyttä tai ympäristöturvallisuutta ***kohtalaisesti*** *.*

Varmistettava korkealla tasolla aina

- Toiminnalle kriittistä, esim. toiminnan keskeytys voi vaarantaa ihmisten terveyden tai turvallisuuden tai keskeytys aiheuttaisi merkittävän taloudellisen, turvallisuus - tai ympäristöriskin
- Ei ole vaihtoehtoista / korvaavaa järjestelyä

Sisältää kaiken sellaisen toiminnan, jonka häiriintyminen tai uhkatilanteet vaarantavat toimintaa, taloutta, asiakassuhteita, terveyttä tai ympäristöturvallisuutta ***merkittävästi*** *.*

Kuva 17: Kolmiportainen luokittelu kohteen kriittisyyden arviointia varten

4.4 KEHÄSUOJAUSMALLI JA VYÖHYKKEET

Kehäsuojausmalli perustuu ajatukseen, että kohteen fyysinen turvallisuus muodostetaan useista peräkkäisistä suojausvyöhykkeistä, jotka vaikeuttavat tunkeutumista ja viivyttävät hyökkääjää. Mallin tavoitteena on luoda kerroksellinen suojaus, jossa jokainen vyöhyke lisää turvallisuustasoa ja tarjoaa mahdollisuuden havaita ja estää uhka ennen kuin se saavuttaa kriittiset kohteet.

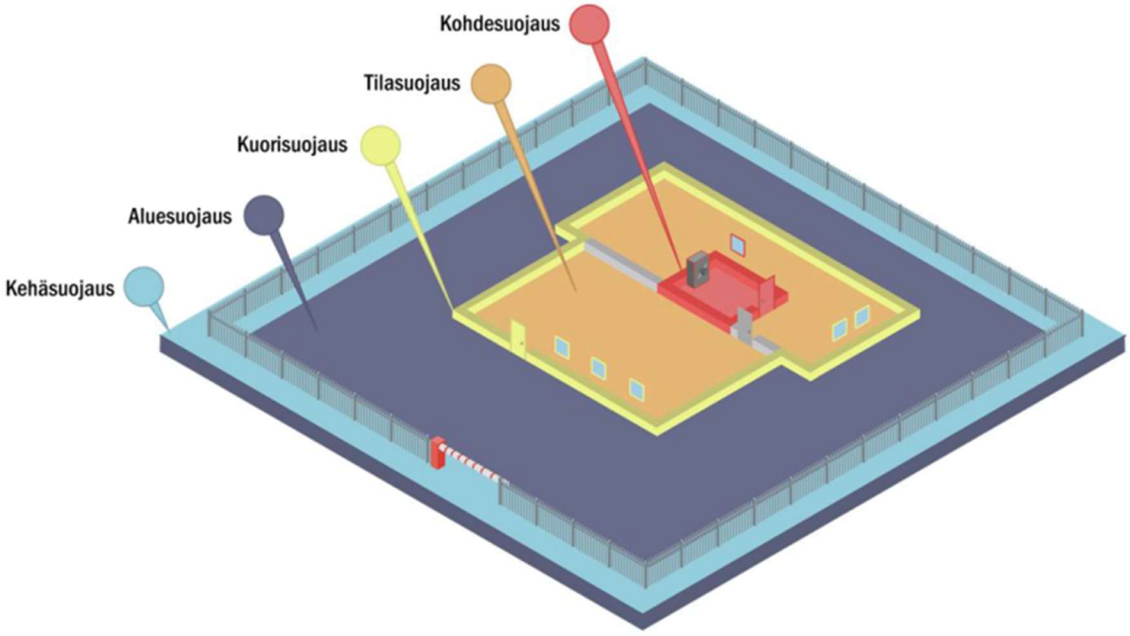
Perusperiaatteet:

1. **Monikerroksisuus**: Turvallisuus ei perustu yhteen esteeseen, vaan useisiin peräkkäisiin kerroksiin.
2. **Viivytys ja havainnointi**: Jokainen vyöhyke hidastaa etenemistä ja mahdollistaa uhkien havaitsemisen.
3. **Vyöhykkeiden erottelu**: Jokaisella vyöhykkeellä on oma turvallisuustaso ja pääsyvaatimukset.

Vyöhykkeet ja niiden tarkoitus (kuva 18 Kehäsuojausmallin vyöhykkeet):

- (Ulko)Kehäsuojaus
  - Ulommainen suojaustaso, joka rajaa kiinteistön tai alueen. Tavoitteena on estää luvaton pääsy ja ohjata kulku hallituille reiteille.
    Esimerkkejä: Aidat, portit, kulunvalvonta, mekaaninen lukitus, kameravalvonta.
- Aluesuojaus
  - Kiinteistön sisäpiha tai rakennusten ympäristö. Täällä tarkennetaan valvontaa ja rajoitetaan liikkumista.
    Esimerkkejä: Liikkumisrajoitukset, valaistus, valvontakamerat.
- Kuorisuojaus
  - Rakennuksen ulkoseinät ja sisäänkäynnit. Kuori estää pääsyn sisätiloihin ja sisältää teknisiä ratkaisuja tunkeutumisen estämiseksi.
    Esimerkkejä: Ovet, ikkunat, luukut, lukitusjärjestelmät, kulunvalvonta, hälytysjärjestelmät.
- Tilasuojaus
  - Rakennuksen sisätilat, joissa sijaitsevat kriittiset toiminnot. Pääsy on rajattu vain valtuutetuille henkilöille.
    Esimerkkejä: Sisäovet, kulkuoikeudet, palo-osastointi, kameravalvonta.
    - Kohdesuojaus
      - Erittäin kriittiset kohteet, kuten prosessinohjausjärjestelmät, SCADA-laitteet ja vedenkäsittelylaitteet.
        Esimerkkejä: Hälytysjärjestelmät, kameravalvonta, henkilökohtaiset käyttäjätunnukset

Kehäsuojausmalli tukee riskienhallintaa, sillä se mahdollistaa uhkien hallinnan vaiheittain ja vähentää riskiä, mikäli yksittäinen suojausratkaisu pettää.



Kuva 18 Kehäsuojausmallin vyöhykkeet

Kehäsuojausmallin periaatteet sekä sovellettavat esimerkit eri kohteiden suojausratkaisuista (kaivot ja vesihuollon liityntäpisteet, vesitorni, pienet syrjäiset kohteet, keskisuuret kohteet ja laitosalueet) on esitetty erillisessä liitteessä ***"Liite 3 – Kehäsuojamallin esimerkkiratkaisut"***. Huomioitavaa on, että esimerkit ovat suuntaa antavia ja todelliset toteutukset tulee aina perustaa erillisiin arviointeihin, kuten riskienarviointiin ja kohteen kriittisyyden arviointiin.

4.5 RAKENTEELLINEN SUOJAUS

Rakenteellinen suojaus kattaa kiinteistöä, rakennusta ja tilaa suojaavat fyysiset esteet, kuten seinät, ovet, ikkunat, lattia- ja kattorakenteet sekä säilytysyksiköt. Näiden rakenteiden tarkoituksena on estää tai hidastaa luvaton pääsy suojattuun kohteeseen niin, että tunkeutuminen ei onnistu havaitsematta määritetyn vasteajan puitteissa tai tunkeutuja luopuu aikeistaan kokonaan. Rakenteellinen suojaus ei rajoitu vain ihmisten aiheuttamien tunkeutumisyritysten estämiseen, vaan sen avulla pyritään myös estämään pieneläinten pääsy vesihuoltokohteisiin, koska ne voivat aiheuttaa rakenteellisia vaurioita, hygieniariskejä ja terveysuhkia. Rakenteiden lisäksi fyysinen suojaus sisältää alueellisia ratkaisuja, kuten aitoja, portteja ja ajoneuvohidasteita, joilla rajataan ja hallitaan liikkumista sekä vähennetään riskiä luvattomasta tunkeutumisesta.

Luvaton tunkeutuminen on rikoslain 24 luvun mukaista julkisrauhan rikkomista. Fyysisillä turvallisuusratkaisuilla, kuten rakenteellisella suojauksella, kulunvalvonnalla ja tilojen käyttörajoituksilla ehkäistään tällaisia rikoksia ja suojataan toiminnan jatkuvuutta.

4.5.1 Aidat

- Aidan tehtävä on rajata alue ja viestiä, että pääsy on luvanvaraista. Sen vaikutus perustuu tunkeutumisyritysten hidastamiseen ja parhaimmillaan ennaltaehkäisyyn. Aitalinja tukee luonnollista valvontaa ja siihen voidaan liittää teknisiä turvajärjestelmiä. Yleensä aitauksen yläosaa ei tarvitse varustaa kiipeilyesteillä tai teknisellä valvonnalla, mutta kriittisillä alueilla tämä voidaan sisällyttää kokonaisratkaisuun.

- Turvallisuustarkoituksessa aidan tulee olla riittävän korkea, lujarakenteinen ja tarvittaessa sisältää elementtejä, jotka vaikeuttavat ylittämistä tai alittamista. Porttien ja puomien on täytettävä samat vaatimukset, jotta aitalinjassa säilyy turvallisuustarkoituksen mukainen yhtenäisyys.
- Lumenkasaantuminen ei saa heikentää aitalinjan toimintaa (aita oltava riittävän korkea huomioiden myös lumenkasaantuminen).
- **Suositellut aidan minimivaatimukset:**
    - Korkeus 2500 mm
    - Materiaali: teräs
    - Kolmilanka-aita 6 mm pysty – 2 x 8 mm vaaka
    - Kiinnitys metallitolppiin, joiden väli korkeintaan 2500 mm
    - Metallitolpat kiinnitetty luotettavasti maahan, joko valulla tai riittävän syvälle kallioon tai muuhun kiinteään materiaaliin
    - **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
        - Vesihuoltolaitokset, jotka sisältävät useampia kohteita laitosalueen sisällä, on ulkoalue suositeltavaa aidata ja rajata oikeudettomien kulkua laitosalueelle.
        - Miehittämättömissä kohteissa, joissa ei ole luonnollista valvontaa, on suositeltavaa aidata kohde ja rajata oikeudettomien kulkua.
        - Myös jo valmiiksi aidattujen alueiden sisäpuolella voidaan tunnistaa sellaisia kohteita, jotka vaativat kohdekohtaisen aidan. Tämä voi tulla kyseeseen, jos kohde on kriittinen ja esimerkiksi ajoneuvolla tapahtuvaa vahingontekoa halutaan estää tai hidastaa.

4.5.2 Henkilöportit

- Aidatulle alueelle kulku mahdollistetaan käyttäen erilaisia henkilö- ja ajoneuvoportteja osana aitarakennetta. Portin avulla alueelle kulku rajataan vain henkilöille, joilla on asianmukainen syy kulkea alueelle. Portin lukituksen ja kulunvalvonnan avulla kulkuliikennettä alueelle tai yksittäiselle kohteelle pystytään rajaamaan ja seuraamaan, sekä hyödyntämään turvateknisen valvonnan rajapintana.
- Porttityypin valinnan tulee ominaisuuksiltaan myötäillä kohteen turvallisuustasoa sekä valittua aitatyyppiä, jotta aitalinjan suojauksen taso olisi yhdenmukainen.
- Esimerkiksi pyöröportilla on mahdollista valvoa laitosalueelle kulkua, koska pyöröportti annostelee kulun siten, että vain yksi henkilö pääsee läpi kerrallaan. Kortinlukijalla tai muilla tunnistimilla varustettuna se varmistaa, että vain luvalliset henkilöt pääsevät laitosalueelle.
- Vierailijoille tarkoitetut portit voidaan varustaa porttipuhelinjärjestelmällä.
- Porttiympäristöissä tulee huomioida myös hätäpoistumistiemääräykset.
- Lumenkasaantuminen tai kertyvä jää ei saa estää porttiympäristön toimintaa. Tämän osalta tulee suunnitella riittävät lumenläjityspaikat vesihuoltolaitoksen tontille ja riittävän etäälle aitalinjasta.
- **Käyntiportti / henkilöportti:**
    - 1-lehtinen käyntiportti (käsikäyttöinen)
    - Kulkuaukon leveys: 1100 – 1200 mm
    - Käyntiportin korkeudet: 2200-2400 mm
- **Pyöröportti:**
    - Kuumasinkitty teräsrakenne
    - Kulkukäytävän leveys min. 60 cm
    - Kiertokulma 120 astetta
    - Optiona kattovalo sekä lämmitys
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**

- Isot vesihuoltokohteet, joissa velvoitettu tunnistamaan ja yksilöimään alueelle tulijat ja alueelta poistujat.

4.5.3 Ajoneuvoportit

- Ajoneuvoporttia valittaessa tulee huomioida aukon leveys, liikenteen määrä, avautumisnopeus, kohteen turvallisuustaso sekä porttiympäristön talvikunnossapito. Yleisimmät ajoneuvoportit ovat liukuportti ja taittoportti, jotka molemmat soveltuvat sekä henkilö- että raskaan liikenteen käyttöön. Portin yhteyteen voidaan asentaa myös puomikoneistoja, jotka nopeuttavat käyttöä erityisesti ruuhka-aikoina.
- Erityisen kriittisissä kohteissa voidaan käyttää myös sulkuporttiratkaisua, joka on kahden portin tai esteen muodostama kulkujärjestely, jossa vain yksi portti voi olla kerrallaan auki. Sen päätarkoitus on hallita ja turvata ajoneuvojen pääsy rajoitetulle tai suojatulle alueelle.
- Lumenkasaantuminen tai kertyvä jää ei saa estää porttiympäristön toimintaa.
- Sähköisen ajoneuvoportin avautuminen tulee varmistaa myös sähkökatkotilanteissa. Avautumista voidaan ohjata esimerkiksi kulunvalvontaan liitettynä, kaukoohjauksella tai etänä.
- **Teräs ja alumiini**
  - Useimmiten portit valmistetaan kuumasinkitystä teräksestä tai vahvasta alumiinista. Näiden materiaalien etuna on pitkä käyttöikä ja erinomainen säänkestävyys.
- **Pinnoitteet ja viimeistelyt**
  - Jauhemaalatut pinnoitteet tarjoavat sekä esteettistä että teknistä hyötyä. Ne suojaavat porttia korroosiolta ja kulumiselta samalla, kun ulkonäkö voidaan sovittaa kohteen ilmeeseen.
- **Testatut rakenteet**
  - Kovaan käyttöön suunnitellut liukuportit testataan standardien mukaisesti. Tämä varmistaa, että ne kestävät sekä sään että mekaanisen rasituksen vuosikymmenien ajan.
- **Kulunvalvonnan integrointi**
  - Kohteiden liukuportit on lähes poikkeuksetta yhdistetty kulunvalvontajärjestelmiin. Korttilukijat, rekisterikilven tunnistus tai RFID-teknologia mahdollistavat sujuvan ja turvallisen sisäänajon ilman manuaalista valvontaa ja mahdollistaa samalla lokitiedot kuluista.
- **Fyysinen este ja rikosten ennaltaehkäisy**
  - Korkeat ja vankkarakenteiset liukuportit toimivat tehokkaana esteenä luvattomalle sisäänpääsylle. Portin runko ja täyte voidaan räätälöidä siten, että se estää myös kiipeämisen
- **Törmäyssuoja ja hätäpysäytys**
  - Ajoneuvoportit sisältävät turvamekanismeja, kuten valokennoja ja törmäyssuojia. Näiden avulla estetään portin sulkeutuminen ajoneuvon tai jalankulkijan päälle. Lisäksi hätäpysäytyspainikkeet parantavat turvallisuutta poikkeustilanteissa.
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
  - Kohteet, joihin toteutettu tai toteutetaan aitarakenne, on suositeltavaa täydentää sitä yhdenmukaisella porttirakenteella. Porttirakenteen valinnassa ja lukitus- tai kulunvalvontaperiaatteissa tulee huomioida mm. se, kuinka aktiivisesti porttia käytetään (esim. aktiivinen laitosalue VS. syrjäinen kohde).

4.5.4 Seinät, katot ja lattiat – rajaavat rakenteet

- Tilaa rajaavat rakenteet, jotka voivat olla kohteen ulkopintoja tai muihin sisätiloihin rajoittuvia seiniä, lattioita tai kattoja. Rakenteiden on kiinnityksineen oltava sellaisia, ettei tilaan pysty tunkeutumaan rakenteita rikkomatta. Rakenteet tai niiden osat eivät saisi myöskään olla ulkopuolelta rikkomatta irrotettavissa.
- Seinä, katto tai lattiarakenteita ei tyypillisesti vahvisteta erikseen turvallisuustason korottamiseksi, mutta korkean turvallisuustason kohteissa se tulee ottaa huomioon.
    - Rakenteiden vahvistaminen on mahdollista esimerkiksi täydentämällä rakennekerroksia teräs- tai kipsilevyillä, joilla pyritään estämään tai vähintäänkin hidastamaan tilaan mahdollisesti kohdistuvia tunkeutumisyrityksiä.
    - Tämä on tyypillistä etenkin kohdesuojauksessa, kun tilassa tiedetään säilytettävän kallisarvoista omaisuutta, suojattavaa tietoa, turvallisuuskriittisiä laitteita ja järjestelmiä tai harjoitettavan kriittistä toimintaa sekä riskienarvioinnin kautta on tunnistettu riski tilaan liittyvässä tunkeutumisessa.
- Etenkin vesihuoltolaitosten rakennukset, jotka ovat laitosalueen ulkopuolella:
    - Tulisi katolle kiipeäminen estää siten, ettei ulkokuoren rakenteita hyödyntämällä voi rakennuksen päälle kiivetä
    - Ulkokuoren materiaali on suositeltavaa olla sellainen, jonka pesu tai ylimaalaus olisi helppoa toteuttaa, jos kohdetta on töhritty.
- Lisäksi on hyvä huomioida, jos vesihuoltolaitoksen kohteessa on tarpeen toteuttaa esimerkiksi kahdennetut sähkönjakelu- ja tiedonsiirtoyhteydet jatkuvuuden varmistamiseksi, on nämä myös kaapeloitava siten, ettei ne ole tahallaan tai tahattomasti helposti rikottavissa (kaapelireitit ja hyllyt sekä niiden fyysinen suojaaminen).
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
    - Esimerkiksi yleisesti valvottujen laitosalueen ulkopuolisten kohteiden seinärakenteet (kuten **kohteet, joiden kautta mahdollisuus vaikuttaa talousveden laatuun**), jotka arvioidaan mahdollisen ilkivallan tai sabotaasin kohteeksi, voidaan suositella varustettavaksi turvaominaisuuksiltaan vahvemmat yhtenäiset seinärakenteet, jolloin ikkunoita on syytä välttää rakenteissa. Tällöin huomioitava myös kohteen oven turvaominaisuudet ja murronkestävyys.

4.5.5 Ajoneuvohidasteet ja -esteet

- Ajoneuvohidasteet ja -esteet ovat rakenteellisia ratkaisuja, joilla hallitaan ajoneuvoliikennettä ja estetään luvaton tai hallitsematon pääsy suojatuille alueille ja suojattavaan kohteeseen.
- Päätavoitteena on hidastaa ajonopeuksia ja vähentää törmäysriskiä, estää läpiajo tai tunkeutuminen kriittisille alueille tai kohteeseen ja ohjata liikenne hallituille reiteille, esimerkiksi porttien tai valvontapisteiden kautta.
- **Kiinteät esteet**
    - Betoniporsaat, pollarit, teräspalkit – soveltuvat pysyvään sulkuun
- **Siirrettävät esteet**
    - Nostettavat pollarit tai puomit – joustava ratkaisu tilapäisiin tarpeisiin
- **Rakenteelliset hidasteet**
    - Töyssyt, korotetut alueet, ajoradan kavennukset – käytetään nopeudenhallintaan
- Ajoneuvohidasteita ja -esteitä on suositeltavaa täydentää heijastimilla tai siten, että ne ovat muutoin helposti havaittavissa.
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**

  - Kriittisten kohteiden läheisyydessä, jotka eivät ole aidattu ja joissa ei muutoin ole mahdollista esimerkiksi ajoneuvoreittiin vaikuttamalla hidastaa ajonopeuksia sekä arvioidaan, että ajoneuvolla voidaan tahallisesti tai tahattomasti aiheuttaa törmäys suojattavaan kohteeseen.

4.5.6 Ovirakenteet

- Ovet tulisi olla rakenteeltaan sellaisia, joista tunkeutuminen ei ole mahdollista ilman työkaluin tapahtuvaa rakenteiden rikkomista. Ovityyppien valinnassa tulee ottaa huomioon suojattavan kohteen turvallisuustaso, johon liittyy olennaisesti myös muu kokonaisuus seinä-, lattia-, katto- ja ikkunarakenteiden vahvuudesta.
  - Ovien osalta tulee huomioida myös saranapuolen suojaus.
- Ovihankinnoissa tulee huomioida, että niille toteutetaan tarvittavat kaapeloinnin edellyttämät työstöt ja varaukset esimerkiksi kulunvalvonta- ja tai murtohälytysjärjestelmää varten, jotta vältytään jälkikäteen tehtäviltä rakenteellisilta muutoksilta. Jälkikäteen tehdyt rakenteelliset muutokset voivat muuttaa oven paloluokitusta.
- Oven rakenteen materiaali vaikuttaa sen turvaominaisuuksien vahvuuteen. Turvaominaisuuksiltaan vahvat ovet ovat tyypillisesti metallisia.
- Ovityypin turvallisuustaso ja sen kyky kestää tunkeutumisyrityksiä määritellään EN 1627 -standardin RC-luokituksilla (RC1–RC6). Mitä korkeampi RC-luokka, sitä paremmin ovi kestää murtotyökaluja ja pidempikestoisia murtoyrityksiä.
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
  - Esimerkiksi yleisesti valvottujen laitosalueen ulkopuolisten kohteiden ovet (kuten vesitornit), jotka arvioidaan mahdollisen ilkivallan tai sabotaasin kohteeksi, voidaan suositella varustettavaksi turvaominaisuuksiltaan vahvempina murtosuojaovina. Tällöin huomioitava myös muu kuorirakenteen kokonaisuus siten, että se on yhtenäinen murtosuojaoven turvallisuustason kanssa.
  - RC2 ja RC3 ovat yleisimmät luokat, joita käytetään kohteissa, joissa vaaditaan selvästi parempaa murtosuojausta kuin tavallisessa rakennusovessa. Tätä korkeamman luokituksen ovia käytetään lähinnä erittäin korkean suojaustason kohteissa.

4.5.7 Ikkunat, aukot ja luukut

- Rakennuksen ikkunat ovat tärkeä suunnitella ja suojata siten, ettei niitä pystytä rikkomatta irrottamaan ulkopuolelta sekä siten, että ne ovat sijoitettuina tarpeeksi korkealle tunkeutumisen todennäköisyyden minimoimiseksi.
- Korkeamman turvaluokan kohteissa tulee harkita murtosuojattujen lasielementtien tarvetta etenkin, jos mahdollinen tunkeutuminen kohteeseen arvioidaan riskiarviossa todennäköiseksi.
- Ikkunoihin liittyen tulee huomioida salakatselun mahdollisuus, ja täten estää näkyvyys etenkin sellaisiin tiloihin, joissa käsitellään salassa pidettäviä aineistoja.
  - Huomioitavaksi, että kaikkiin kohteisiin ei ole tarkoituksenmukaista toteuttaa ikkunoita ollenkaan. Tällä ratkaisulla on mahdollisuus hidastaa tai kokonaan estää mahdollinen tunkeutumisyritys kohteeseen tai ikkunoihin liittyvä ilkivalta.
  - Ikkunoita on kuitenkin erilaisia vahvuustyyppejä tai niitä on mahdollisuus vahventaa erilaisilla suojakalvoilla. Lisäksi ikkunoita on mahdollista valvoa turvatekniikan avulla.
- Rakennuksessa olevat aukot kuten esimerkiksi katto- ja ilmastointiluukut tulee suunnitella siten, että kulku näiden aukkojen ääreen tapahtuu vain valvotuista tiloista. Vaihtoehtoisesti aukot suojataan esimerkiksi teräksisin kalterein.

    - Aukkoja ja luukkuja on mahdollista valvoa turvatekniikan avulla.
    - Luukkujen osalta tulee huomioida myös saranapuolen suojaus.
- Ikkunoissa ja aukoissa käytettävä standardi on SFS-EN 1627.
- Lisäksi aukkojen ja luukkujen osalta tulee huomioida esimerkiksi jyrsijöiden ja pieneläimien tunkeutumisen estäminen, koska ne voivat aiheuttaa rakenteellisia vaurioita, hygieniariskiä ja toiminnan keskeytymistä. Kyseistä riskiä voi hallita mm. seuraavin keinoin:
    - Tiheäsilmäisten metalliverkkojen (ruostumaton teräs, joka kestää jyrsintää) asennus luukkuihin, tuuletusaukkoihin tai kaapeliläpivienteihin
    - Ovien ja luukkujen tiivistys hyödyntäen harjalistoja, metallipeltejä ja tiivistemassoja, jolloin pienetkin raot saadaan umpeen
    - Yleinen rakenteiden, suojaverkkojen ja tiivisteiden tarkastus ja kunnossapito, jolloin mm. havaitut halkeamat ja raot korjataan tai suojataan
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
    - Etenkin kohteet, joiden kautta on mahdollisuus vaikuttaa talousveden laatuun, tulee erityisesti suojata eläinten aiheuttamilta terveys- ja hygieniariskeiltä sekä asiattomien tunkeutujien aiheuttamilta sabotaasi- tai ilkivaltariskeiltä.

4.5.8 Valaistus

- Riittävän voimakas, tasalaatuinen sekä muilta ominaisuuksiltaan sijoitettavaan toimintaympäristöön tarkoituksenmukainen valaistus on yksi keskeisistä rakenteellisen suojauksen komponenteista. Valaistus on sellaisenaan tehokas keino muun muassa rikollisuuden sekä vaaratilanteiden ehkäisemiseksi. Merkittävä vaikutus sillä on etenkin tapaturmien ennaltaehkäisemisessä.
- Lisäksi valaistusta voidaan hyödyntää tehokkaasti osana muita turvajärjestelmiä integraatioiden avulla esimerkiksi niin, että murtoilmaisu- tai kulunvalvontajärjestelmän hälytys ohjaa valaistuksen hälyttäville alueille, mikä voi osaltaan häiritä mahdollista tunkeutujaa tai jopa saada tämän perääntymään aikeistaan.
- Voidaan toteuttaa myös liiketunnistukseen tai hämäräkytkimeen perustuen.
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**
    - Valaistus on verrattain kustannustehokas tapa toteuttaa fyysisen turvallisuuden tukitoimintoja ja sitä onkin suositeltavaa hyödyntää monenlaisissa kohteissa ja laitosalueella. Etenkin kohteissa, joissa ei ole aktiivista toimintaa tai kulkua, on valaistusta suositeltavaa ohjata liiketunnistukseen perustuen.

4.5.9 Kyltit sekä kielto- ja varoitusmerkit

- Kylttien tehtävä on ennaltaehkäistä oikeudetonta kulkua ja ohjata liikkumista laitoksen alueella tai suojattavan kohteen läheisyydessä. Ne eivät fyysisesti estä tunkeutumista, mutta toimivat selkeänä viestinä alueiden rajoista, käyttöoikeuksista ja riskeistä. Näin ne tukevat fyysisiä suojauskeinoja (kuten aidat) ja turvajärjestelmiä.
- Tarkoituksena:
    - Alueiden rajojen korostaminen ja kulun ohjaus
    - Kameravalvonnasta ilmoittaminen (lakisääteinen velvoite)
    - Riskien ja vaarojen ennalta ehkäisy
- Käytä selkeitä symboleja ja standardoituja värejä (punainen = kielto, keltainen = varoitus, sininen = ohje).
- Sijoita kyltit näkyville paikoille, kuten sisäänkäynteihin, portteihin ja riskialueiden rajalle.
- Huolehdi kylttien ajantasaisuudesta ja kunnosta.
- **Suositus minkälaiseen vesilaitoskohteen ympäristöön sovellettavissa:**

  - Laitosalueen rajat tulisi selkeästi merkitä ohjaus- tai kielto- ja varoituskyltein
  - Kaikki kohteet tai alueet, jossa kameravalvontaa toteutetaan, tulee siitä ilmoittaa kyltein

Tiivistetysti: Rakenteellisen suojauksen periaatteet

- **Tarkoitus:** Fyysisen turvallisuuden tavoitteena on estää, hidastaa ja havaita luvaton pääsy suojattuihin alueisiin ja tiloihin sekä ehkäistä pieneläinten pääsy vesihuoltokohteisiin, koska ne voivat aiheuttaa terveys- ja hygieniariskejä.
- **Rakenteellinen suojaus:** Materiaalivalinnat tai käytettyjen rakenteiden vahvistaminen toteutetaan siten, että tunkeutuminen vaatii työkaluja ja aikaa. Rakenteellinen suojaus toteutetaan niin, että se estää myös eläinten ja pieneläinten kulkeutumisen vesihuoltokohteeseen.
- **Alueelliset ratkaisut:** Aidat, portit, ajoneuvohidasteet sekä ohjauskyltit rajaavat ja ohjaavat liikkumista sekä vähentävät riskiä luvattomasta tunkeutumisesta.
- **Valaistus:** Riittävä ja oikein sijoitettu valaistus tukee valvontaa ja vähentää rikos-, tapaturma- ja ilkivaltariskejä.
- **Kehäsuojausmalli:** Vyöhykkeellinen rakenteellinen suojaus toimii parhaiten yhdessä teknisten turvajärjestelmien kanssa.
- **Periaate:** Kaikki rakenteelliset suojausratkaisut suunnitellaan riskiperusteisesti ja ne muodostavat yhtenäisen, tarkoituksenmukaisen kokonaisuuden.

4.6 TURVATEKNIIKAN JÄRJESTELMÄT

Etenkin kohteet, joissa voidaan olettaa, että vasteaika on hyvinkin pitkä *(miehittämättömät kohteet, kohteen fyysinen sijainti jne.)*, tulee huomioida sellaisen turvatekniikan valinta, jolla voidaan todentaa kohteen tila tai hälytyksen aiheuttama tekijä. Esimerkiksi kameravalvontajärjestelmällä on mahdollisuus reaaliaikaisesti tai jälkikäteen todentaa häiriön aiheuttaja ja se onkin suositeltava valvontakeino, jos se on mahdollista toteuttaa kustannustehokkaasti (mm. sähkönsyöttö, tietoliikennevaatimukset). Aikaleiman käyttö tallennuksessa on olennaisen tärkeä apuväline poikkeamien selvityksessä. Lisäksi erilaisilla hälytysjärjestelmillä on mahdollisuus todentaa kohteen tila ja hälytykset on mahdollista siirtää oman vesihuoltolaitoksen yhteyshenkilöiden lisäksi palveluntarjoajalle, joka voi hälytyksen tullessa käydä tarkastamassa kohteen tilan, jos näin on velvoitettu.

4.6.1 Kameravalvontajärjestelmät

- Kameravalvontajärjestelmän tarkoituksena on valvoa sille ennalta suunniteltuja valvonta-alueita tai kohteita. Kameravalvontaa voidaan hyödyntää turvallisuustapahtumiin liittyvän valvonnan lisäksi vesihuolto- ja jätevedenpuhdistusprosessien valvonnassa sekä analytiikan tuottamisessa. Valvonta-alue suunnitellaan riskiperusteisesti kohteen käyttötarkoitus, luonne ja suojattavat arvot huomioiden.
- Kameravalvontajärjestelmä koostuu tyypillisesti:
  - tallentimesta tai videohallintaohjelmistosta,
  - verkkokytkimistä sekä
  - valvontakameroista.
- Kameravalvontajärjestelmään liittyvien laitteiden valinnassa, sekä niihin liittyvien teknisten vaatimusten määrittelyssä on tärkeää huomioida toimintaympäristöön liittyvät muuttujat, kuten esimerkiksi:
  - sää- ja valoisuusolosuhteet,
  - ympäristö ja kasvillisuus,
  - valvonta-alueen laajuus,
  - tarvittava valvontakuvan tarkkuus (yleiskuva/tunnistuskuva/yksilöintikuva).

- Kameravalvontajärjestelmän päätarkoituksena on saada joko reaaliaikaista tai tallentavaa (tai molempia) kuvamateriaalia määritellyltä alueelta. Kuvaa hyödynnetään tyypillisesti turvallisuustapahtumiin reagoimiseksi. Kuvan antaman tilannetiedon perusteella voidaan esimerkiksi lähettää tapahtumapaikalle vartiointiliikkeen edustaja. Tallennemateriaalia voidaan hyödyntää tapahtumaketjujen selvittämiseen ja todentamiseen jälkikäteen.
- Kameravalvonnassa voidaan hyödyntää mm. seuraavia ominaisuuksia tai laitteistoja:
    - Kiinteä kamera (kuvaa määritettyä valvonta-aluetta)
    - PTZ-kamera (liikuteltava, etäohjattava kamera – voidaan määrittää esim. automaattisia valvontakierroksia)
    - IR-kamera (infrapunakamera, ”lämpökamera” – voidaan hyödyntää erityisesti mm. pimeässä tai haastavissa sääolosuhteissa. Voidaan yhdistää tavalliseen valvontakamerakuvaan, jolloin saadaan sekä visuaalinen että lämpökuva)
    - ANPR-kamera (rekisterikilventunnistuskamera)
    - Radar (valvontakameran rinnalla käytettävä tutka (radar, lisälaite), jonka tarkoituksena on havaita liikettä ja kohteita myös olosuhteissa, joissa valvontakameran näkyvyys on heikko (esim. pimeys, sumu, sade))
    - Drone (liikkuva valvontayksikkö). Suomessa on käytössä droneja sekä robottikoptereita, joita voidaan käyttää liikkuvina valvontakameroina. Ihmisen on ohjattava kumpaakin laitetta.
        - Dronea ohjataan tyypillisesti ohjaimen avulla, robottikopteria taas on mahdollista valvoa myös etänä.
        - Robottikopteri eroaa droneista sillä, että sen avulla on mahdollista seurata havaittuja droneja ja vaikuttaa niiden liikkeisiin signaalihäirinnällä.
        - Suomen lainsäädäntö ei toistaiseksi mahdollista muunlaista vaikuttamista (esim. pudottaminen, verkon heittäminen dronen päälle).
        - Lentävien laitteiden käytössä on huomioitava, että niiden käyttöön liittyy tiettyjä rajoitteita eikä kaikilla alueilla saa niitä lennättää. Traficomin Droneinfo-sivusto tarjoaa kattavasti tietoa aiheesta.
    - Analytiikka (Ohjelmistoja ja algoritmeja, jotka käsittelevät kameran tuottamaa kuvaa automaattisesti ja tuottavat siitä hyödyllistä tietoa. Tarkoitus on parantaa valvonnan tehokkuutta ja vähentää manuaalista työtä.)
        - Hyödynnettävissä esimerkiksi virtuaaliaitojen luomisessa
    - Puhe-/kuulutusyhteys valvottavaan kohteeseen, jonka avulla mahdollisuus reagoida välittömästi kameravalvonnalla havaittuun poikkeavaan tilanteeseen, kuten tunkeutumisyritykseen.
- Valvonta-alueet
    - Yleiskuvan kameralla on tarkoitus kuvata nimensä mukaisesti yleisesti aluetta, joka halutaan kameravalvonnan piiriin. Esimerkiksi:
        - Kiinteistöjen ulkokuori ja sen seinustat
        - Laajat piha- sekä pysäköintialueet
    - Tunnistuskuvan kameran tarkoituksena on havaita valvotulla alueella sellaisella tarkkuudella tapahtuva asia, henkilö, esine tai ajoneuvo, jotta valvontakuvan perusteella voidaan tunnistaa esimerkiksi vaatetuksen väri sekä tapahtumien tarkka kulku. Esimerkiksi:
        - Käytävät
        - Sisäänkäyntien edustat
        - Kriittisten kohteiden tai tilojen välitön läheisyys
    - Yksilöintikuvalla tarkoitetaan kameraa, jonka tekniset ominaisuudet mahdollistavat tarkan valvontakuvan halutusta valvonta-alueesta siten, että valvonta-alueella liikkuvat henkilöt sekä ajoneuvot voidaan yksilöidä.

        - Henkilö- ja ajoneuvoportit
        - Kriittisten kohteiden sisäänkäynnit
- Tietosuoja-asetuksen huomioiminen kameravalvonnassa
    - Kameravalvonnasta tulee ilmoittaa
    - Kameravalvontaan liittyen tulee tuottaa kirjallinen kuvaus vesihuoltolaitoksen tekemästä henkilötietojen käsittelystä, eli *rekisterinpitäjän seloste käsittelytoimista*. Seloste käsittelytoimista tulee tehdä aina, kun henkilötietojen käsittely ei ole satunnaista.
    - Seloste on laitoksen sisäinen asiakirja, eikä se ole suoraan tarkoitettu käytettäväksi rekisteröityjen informointiin, mutta sitä voidaan hyödyntää rekisteröidyille suunnatun informaation tuottamisessa.
    - Rekisterinpitäjä on kameravalvontajärjestelmän ”omistaja”, eli useimmiten kameravalvonnan toteuttamisesta vastaava vesihuoltolaitos, ja täten päävastuussa henkilötietojen käsittelyn lainmukaisuudesta ja yksilöiden oikeuksista.
    - Kameravalvonnan toteuttamista ohjaa useat lait, joihin on viitattu myös oppaan erillisessä liitteessä ***”Liite 1 – Ohjaavat muut asiakirjat”***.

Tiivistetysti: Kameravalvontajärjestelmät
- **Tarkoitus:** Kameravalvonta valvoo ennalta määriteltyjä alueita turvallisuuden ja prosessien hallinnan tueksi.
- **Rakenne:** Järjestelmä koostuu tallentimesta/videohallintaohjelmistosta, verkkokytkimistä ja kameroista, joiden valinta perustuu riskiperusteiseen suunnitteluun ja olosuhteisiin.
- **Käyttö:** Tuottaa reaaliaikaista tai tallennettua kuvaa tapahtumiin reagoimiseksi ja jälkiselvityksiin.
- **Tehostaminen:** Erilaiset kameratyypit, lisälaitteet (esim. PTZ-, IR-, ANPR-kamerat, dronet) ja analytiikka parantavat valvonnan tarkkuutta ja tehokkuutta.
- **Lakisääteisyys:** Toteuttamista ohjaa mm. Yleinen tietosuoja-asetus (GDPR), Tietosuojalaki, Laki yksityisyyden suojasta työelämässä.

4.6.2 Kulunvalvontajärjestelmät

- Kulunvalvontajärjestelmä on tilaturvallisuusjärjestelmä, jonka tarkoitus on määritellä kulkuoikeudet henkilöille kiinteistössä liikkumiseksi, sekä estää luvattomien henkilöiden pääsy suojattuun tilaan. Lisäksi järjestelmällä on mahdollista valvoa ovien tilaa (auki/kiinni) yhdessä rikosilmoitinjärjestelmän kanssa.
- Kulunvalvontajärjestelmän aktiivinen, ajantasainen ja ammattitaitoinen hallinnointi vaikuttaa merkittävästi kulunvalvontajärjestelmän vaikuttavuuteen.
- Järjestelmän hallinnointiohjelmistossa voidaan laatia kulkuoikeusryhmiä ja -alueita, nimetä eritasoisia oikeuksia henkilöille, valvoa lokitietoja ovien menneistä kuluista sekä valvoa ovien tilatietoa ja asettaa oville aikaohjelmia. Aikaohjelmilla määritellään esimerkiksi se, milloin ovien kulku aiheuttaa hälytyksen tai onko ovien moottorilukko tarvetta avata kokonaan pääsyn helpottamiseksi.
- Kulunvalvontajärjestelmä koostuu tyypillisesti:
    - Palvelimesta, tai useammasta yhdistetystä palvelimesta
    - Keskuslaitteesta, eli väyläohjaimesta
    - Ovikohtaisista ovi/pääteohjaimista
    - Kulunvalvonnan lukijoista
    - Kulkutunnisteista ja avaimista
    - Kytkimistä
- Kulunvalvonnassa voidaan hyödyntää mm. seuraavia laitteita tai ominaisuuksia:

  - Tavallinen kulunvalvontalukija
  - PIN-koodilukija (2-vaiheinen tunnistautuminen: kulkutunniste & PIN-koodi – suositeltava etenkin ulkokuorella ja kriittisissä kohteissa)
    - PIN-koodilukijat voidaan varustaa näkösuojauksella, jonka tarkoituksena on estää asiattomia näkemästä näppäiltävää koodia
  - Biometriset lukijat (kulkuoikeus todennetaan biometrisen tunnisteen, kuten sormenjäljen-, äänen-, iiriksen-, kasvojen rakenteen tai kämmenen verisuonten avulla. Huomioitava mm. korkeammat kustannukset perinteisiin lukijoihin verrattuna ja GDPR-vaatimukset)
  - Kulkutunniste, esimerkkejä:
    - Fyysinen kulkutunniste, kuten kortti tai tägi
    - Mobiiliavaus (puhelimeen liitetty)
    - Biometrinen tunniste
  - Salausteknologia (tunnistiminen ja lukijoiden sekä lukijan ja keskuslaitteen välinen viestintä on salattua salausavaimella)
- Huomioitava lukijoiden valinnassa
  - Nykyaikainen teknologia
  - Organisaatiokohtaiset applikaatiot (salaustiedostot)
  - Riittävä salaus (vähintään AES 128)
  - Soveltuvuus käyttöympäristöön (IP- ja käyttölämpötilat)
  - Asennusmahdollisuudet (ovi- vai seinäpintaan)
- Tietosuoja-asetuksen huomioiminen kulunvalvonnassa
  - Kulunvalvontaan liittyen tulee tuottaa kirjallinen kuvaus vesihuoltolaitoksen tekemästä henkilötietojen käsittelystä, eli *rekisterinpitäjän seloste käsittelytoimista*. Seloste käsittelytoimista tulee tehdä aina, kun henkilötietojen käsittely ei ole satunnaista.

Tiivistetysti: Kulunvalvontajärjestelmät

- **Tarkoitus:** Kulunvalvonta määrittelee kulkuoikeudet ja estää luvattoman pääsyn suojattuihin tiloihin. Lisäksi voidaan valvoa ovien tilaa ja yhdistää se rikosilmoitinjärjestelmään. Mahdollisuus luoda aikaohjelmia ovien auki- ja kiinniololle.
- **Hallinta:** Ajantasainen ja ammattitaitoinen hallinnointi on keskeistä järjestelmän tehokkuudelle. Ohjelmistossa voidaan luoda kulkuoikeusryhmiä, hallita lokitietoja ja asettaa aikaohjelmia ovien toiminnalle.
- **Rakenne:** Järjestelmä koostuu palvelimista, keskuslaitteista, ovikohtaisista ohjaimista, lukijoista, kulkutunnisteista ja kytkimistä.
- **Tunnistautuminen:** Käytössä voi olla mm. PIN-koodit, biometriset tunnisteet, erilaiset fyysiset kulkutunnisteet ja mobiiliavaus sekä monivaiheinen tunnistautuminen.
- **Lakisääteisyys:** Tietosuoja-asetuksen mukainen seloste käsittelytoimista tulee tehdä aina, kun henkilötietojen käsittely ei ole satunnaista.
- **Virtalähteen tarve:** Järjestelmä tarvitsee virtalähteen. Varavoimaratkaisu pidentää käyttöaikaa sähkökatkon sattuessa. Osa järjestelmistä toimii sähkökatkon aikana offline-tilassa ja sallii kulkemisen rajatulle määrälle tunnisteista, joilla on hiljattain kuljettu ovista. Virran loppuessa ovien lukitus toimii ennalta määritettyjen asetusten mukaan (avautuu / pysyy sähköjen katketessa). Varautumisen kannalta on tärkeää selvittää ennalta pääkäyttäjältä/järjestelmän asentajalta, miten järjestelmä on ohjattu toimimaan ja huomioida se suunnitellessa liikkumista häiriötilanteen aikana.

4.6.3 Murtohälytysjärjestelmät

- Murtohälytysjärjestelmä on yleistermi järjestelmälle, joka havaitsee murron, ilkivallan tai muun hälytettävän tapahtuman. Murtohälytysjärjestelmä tunnetaan myös termeillä:
    - Rikosilmoitinjärjestelmä
    - Tunkeutumisen ilmaisujärjestelmä
    - Murtoilmaisujärjestelmä
    - Hälytysjärjestelmä
- Päätarkoituksena on valvoa tilaa, rakennusta, aluetta tai aitalinjaa erilaisin ilmaisimin. Järjestelmän käyttö perustuu hälytyksen ilmaisuun ja hälytyksen siirtoon.
- Hälytystiedolla on mahdollista laukaista murtohälytysjärjestelmään kytkettäviä sireenejä, turvavalaistuslaitteita tai muita laitteita, joilla saadaan aikaan paikallinen hälytys.
- Murtohälytysjärjestelmän ilmaisimista voidaan välittää hälytystieto järjestelmää valvovalle taholle, kuten esimerkiksi vartioimisliikkeelle tai paikalliselle valvomolle.
- Järjestelmä koostuu tyypillisesti:
    - keskuslaitteesta,
    - hälytyksensiirtolaitteesta ja
    - ilmaisinkannasta, kuten:
        - liikeilmaisin,
        - kuunteleva lasirikkoilmaisin,
        - runkoääni- ja tärinäilmaisimet,
        - vesivuotoilmaisimet,
        - ryöstö- ja hätäkutsuilmaisimet,
        - linjailmaisimet,
        - aitavalvontajärjestelmät.
        - lidar-tutkat,
        - sireenit ja vilkut
- Murtohälytysjärjestelmässä voidaan hyödyntää mm. seuraavia laitteita tai ominaisuuksia:
    - Magneettikosketin (ovien, porttien, ikkunoiden ja rakenteellisten aukkojen kuten huolto- ja savunpoistoluukkujen auki-/kiinniolon valvonta)
    - Liikeilmaisin (antaa hälytyksen valvottavassa tilassa tapahtuvasta liikkeestä – reagoi liikkuvaan lämmönlähteeseen (passiivinen infrapunailmaisin) tai reagoi ilmaisinparin välillä kulkevien mikroaaltojen katkeamiseen (mikroaaltoilmaisin) tai yhdistelmäilmaisimet.
    - Lasirikkoilmaisin (antaa hälytyksen ikkunan tai muun lasirakenteen rikkoutumisesta)
    - Aitalinjailmaisimet (usein toteutettuna joko maan alla, sen pinnalla tai aitaan kiinnitettynä kulkevalla kaapelilla, jonka ylittämisestä muodostuu hälytys, tai vaihtoehtoisesti linjailmaisinpareilla, jotka reagoivat infrapunalla tai mikroaalloilla muodostettavan linjan katkeamiseen)
- Murtohälytysjärjestelmät luokitellaan standardin SFS-EN 50131 mukaan luokkiin 1–4. Luokissa 1–2 saa hyödyntää kauttaaltaan langattomia ilmaisimia. Luokassa 3 langattomia ilmaisimia saa hyödyntää ainoastaan kohdevalvonnassa ja hälytyspainikkeissa. Luokassa 4 langattomia ilmaisimia ei sallita.
    - Vesihuollon perustason kohteissa suositellaan vähintään EN50131 luokka (grade) 2 murtoilmaisujärjestelmää.
    - Vesihuollon korotetun tason kohteissa suositellaan vähintään EN50131 luokka (grade) 3 murtoilmaisujärjestelmää.

Tiivistetysti: Murtohälytysjärjestelmät

- **Tarkoitus:** Valvoo tiloja, rakennuksia, alueita tai aitalinjoja ilmaisimilla ja välittää hälytyksen eteenpäin. Hälytys voi laukaista sireenejä, turvavalaistusta tai muita paikallisia hälytyslaitteita.
- **Hälytyksen siirto:** Hälytystieto voidaan välittää valvovalle taholle, kuten vartioimisliikkeelle tai paikalliselle valvomolle.
- **Rakenne:** Järjestelmä koostuu keskuslaitteesta, hälytyksensiirtolaitteesta ja ilmaisimista.
- **Ilmaisintyypit:** Esimerkiksi magneettikosketin (ovet, ikkunat, luukut), liikeilmaisin (lämpö/mikroaallot), lasirikkoilmaisin sekä aitalinjailmaisimet (kaapeli- tai infrapuna-/mikroaaltolinja).

4.6.4 Elektromekaaniset lukitusjärjestelmät

- Kevyt kulunhallinta- ja lukitusjärjestelmä, jonka avulla mahdollistetaan kulkuoikeuksien hallinta sekä lokitietojen kerääminen ovista kulkemisesta
    - Mahdollistaa valmistajasta ja toteutustavasta riippuen ovien tilatiedot, kulkutapahtumista lokitiedot sekä keskitetyn avainten kulkuoikeuksien hallinnan verkkokäyttöliittymän kautta.
- Tyypillisesti Suomen markkinoilla saatavilla olevissa elektromekaanisissa lukitusjärjestelmissä on seuraavat ominaisuudet:
    - Ilman sähköä toimivat avainpesät
    - Lukoston hallinta digitaalisen ohjelmiston kautta.
- Pääkäyttäjä pystyy hoitamaan suurimman osan lukoston hallinnointiin liittyvistä tehtävistä.
    - Avausvälinevaihtoehtoja ovat perinteisen fyysisen älyavaimen lisäksi älypuhelinsovellus, kulkutunniste ja PIN-koodi.
    - Kadonneet avaimet voidaan deaktivoida, jolloin lukitukset eivät vaadi korkeakustanteista uudelleensarjoittamista.
    - Avaimiin asetettuja kulkuoikeuksia on helppo muuttaa, joten avainten kulkuoikeuksien päivittäminen tai vaihtaminen käyttäjältä toiselle onnistuu vaivatta paikasta riippumatta älypuhelinsovelluksen kautta
    - Avainten kulkuoikeuksien päivitys on mahdollista myös manuaalisella avainhallintapisteellä, seinään kiinnitettävässä yksikössä ja käyttämällä päivittävää lukijaa.
    - Elektromekaaniset avaimet eivät yleensä vaadi virtalähdettä, joskin osa toimii paristolla.
- Riippulukkoja on myös saatavilla elektromekaanisella lukitusjärjestelmällä. Tällöin koko laitoksen lukituskanta on mahdollista päivittää yhteneväiseksi, mikä on suositeltavaa etenkin laajemmissa laitoskokonaisuuksissa.

4.6.5 Mekaaniset lukitusjärjestelmät

- Mekaaniset lukitusratkaisut ovat hankintakustannukseltaan edullisin tapa toteuttaa lukitusratkaisu verrattuna kulunvalvontajärjestelmiin ja elektromekaanisiin lukitusjärjestelmiin. Lukitusratkaisu ei vaadi erillisiä lisenssejä, kaapelointeja tai virtalähteitä toimiakseen.
- Mekaaninen avainpesä on mahdollista varustaa ovikytkimellä, jolloin saadaan tieto onko ovi auki vai kiinni. Ovikytkin ei kuitenkaan anna tietoa siitä kuka on ovesta kulkenut.
- Vaatii manuaalista hallinnointia, eli erillisen kirjanpidon jokaisen avaimen haltijasta sekä avainten sarjoituksen eri lukkoihin.

- Mikäli avaimen haltija kadottaa avaimensa, kasvaa riski lukituksen eheydestä, kadotetun avaimen väärinkäytön vuoksi.
    - Uusien avainten tilaus sekä olemassa olevien lukkojen uudelleensarjoitus vaativat aina tilauksen tehtaalta sekä lukkosepän suorittaman asennustyön.
    - Mekaanisen järjestelmän avaimen katoaminen tarkoittaa aina olemassa olevien lukkojen uudelleensarjoitusta kulkemisen estämiseksi eli käytännössä lukkosepän käyntiä kohteella.
- Huomioitava, että mekaaniseen lukitusratkaisuun liittyy sen patentin voimassaoloaika.
    - Patenttisuojauksen päättyminen tarkoittaa sitä, että vanhentuneen lukoston avaimia on mahdollista kopioida malliavaimen perusteella esimerkiksi suutarilla, jolloin avainhallinnan kontrolli katoaa eikä voida varmuudella tietää, kuinka paljon kohteiden avaimia on käytössä ja minkälaisilla tahoilla niitä on hallussa.
- Lukitustekniikka on vuosien aikana kehittynyt, minkä takia vanhimpia lukkoja (ennen vuotta 2010 asennettuja) ei välttämättä ole mahdollista päivittää suoraan moderniin lukitusjärjestelmään johtuen eri ikäisten järjestelmien yhteensopivuuseroista. Käytännössä tämä voi tarkoittaa sitä, että oven lukituspisteen koko varustelu (lukkorunko, avainpesä, painikkeet, mahdollinen oven työstö) tai jopa koko ovi on vaihdettava. Lisäksi on syytä huomioida ovet, joissa mahdollisesti voi olla asbestia. Tällaisten ovien turvallinen työstö vaatii erityistä ammattiosaamista.
- Ennen lukitusjärjestelmien saneerausta on tärkeää kartoittaa kaikkien uusittavien lukituspisteiden määrä ja niiden varustelun nykytilanne, kuten:
    - ovimalli (umpiovi/profiiliovi/palo-ovi)
    - oven kunto
    - oven nykyisen lukkorungon ja avainpesän malli
    - avainpesien puoleisuus (yksi- vai kaksipuoleinen)
    - oven avaustoiminto (painike vai vedin)
    - mahdolliset varmuuslukot

Lukitusjärjestelmien keskeiset erot

- **Hallinta:** Elektromekaaninen tarjoaa digitaalisen ja keskitetyn hallinnan, mekaaninen vaatii manuaalista kirjanpitoa.
- **Tieto ja seuranta:** Elektromekaaninen kerää lokitietoja ja ovien tilatietoja, mekaaninen ei.
- **Joustavuus:** Elektromekaaninen mahdollistaa kulkuoikeuksien nopean muokkauksen ja avainten kuolettamisen, mekaaninen vaatii fyysisiä toimenpiteitä ja uudelleensarjoittamista.
- **Kustannukset:** Mekaaninen on hankinnassa edullisempi, mutta ylläpidossa riskialttiimpi; elektromekaaninen vaatii enemmän investointia, mutta vähentää hallinnollisia riskejä.
- **Virtalähteen tarve:** Järjestelmästä riippuen elekromekaaniset avaimet joko saavat tarvitsemansa virran toimii lukon avausliikkeestä tai toimivat paristolla. Tämä pätee myös lukkopesiin; osa toimii ilman sähköä, online-lukijat ja koodilukot tarvitsevat virtalähteen. Virrattomat lukkopesät ja avaimet toimivat myös sähkökatkon aikana, sähkötoimisen lukon toimintaa voi turvata akkuvarmennuksella. Varautumisen kannalta on tärkeää selvittää ennalta pääkäyttäjältä/järjestelmän asentajalta, miten järjestelmä on ohjattu toimimaan ja huomioida se suunnitellessa liikkumista häiriötilanteen aikana.

Lukitusjärjestelmän valintaan vaikuttavat lukittavan kohteen kriittisyys, lukon arvioidut käyttömäärät sekä kohteen sijainti.

4.6.6 IoT-sensorit

- IoT-sensoreiden tarkoituksena on valvoa ennalta määriteltyjä kohteita ja olosuhteita sekä havaita turvallisuuteen liittyviä poikkeamia kustannustehokkaasti. Niitä voidaan hyödyntää esimerkiksi luukkujen, ovien ja porttien kiinni- tai aukiolon valvonnassa, jolloin voidaan korvata tai täydentää perinteisiä kaapeloituja murtoilmaisujärjestelmiä.
- Lisäksi sensoreita voidaan käyttää vesihuolto- ja jätevedenpuhdistusprosessien seurannassa, ympäristöolosuhteiden valvonnassa sekä analytiikan tuottamisessa. Valvonta toteutetaan riskiperusteisesti kohteen käyttötarkoitus, kriittisyys ja toimintaympäristö huomioiden.
- IoT-sensorijärjestelmä koostuu tyypillisesti:
    - Sensoreista, jotka mittaavat tai havaitsevat esimerkiksi:
        - Luukun tai oven asennon (kiinni/auki)
        - Lämpötilan, kosteuden, paineen, virtausnopeuden
        - Veden laadun (pH, sameus, johtokyky)
    - Tietoliikennekomponenteista (esim. LoRaWAN, NB-IoT, Wi-Fi)
    - Tietojen keruu- ja hallintajärjestelmästä (gatewayt, pilvipalvelut, analytiikkaohjelmistot)
- Sensorien valinnassa ja teknisten vaatimusten määrittelyssä on tärkeää huomioida:
    - Valvottavan kohteen luonne (esim. kriittinen luukku, portti, tekninen tila)
    - Sää- ja ympäristöolosuhteet (lämpötila, kosteus, korroosioriski)
    - Tietoliikenneyhteyksien luotettavuus ja kantama
    - Virransyöttö ja huoltoväli (paristokäyttöiset vs. verkkovirta)
    - Tarvittava reagointinopeus ja hälytysjärjestelmän integraatio.

Tiivistetysti: IoT-sensorit

- **Tarkoitus:** IoT-sensorit valvovat kriittisiä kohteita ja havaitsevat poikkeamia, kuten luukkujen kiinni-/aukiolon, kustannustehokkaasti verrattuna kaapeloituun murtoilmaisujärjestelmään.
- **Hallinta:** Sensorit välittävät tiedon langattomasti hallintajärjestelmään (esim. pilvipalvelu tai valvomo), jossa dataa hyödynnetään hälytyksiin, analytiikkaan ja tilannekuvan ylläpitoon.
- **Rakenne:** Järjestelmä koostuu sensoreista (esim. asento-, lämpötila-, kosteusanturit), langattomasta tiedonsiirrosta (esim. LoRaWAN) ja tietojen hallinta- sekä hälytysjärjestelmästä.
- **Keskeiset huomioitavat tekijät:** Kohteen kriittisyys, ympäristöolosuhteet, tietoliikenneyhteyksien luotettavuus ja virransyöttö.
- **Hyödyt:** Tilannetieto, automaattiset hälytykset ja joustava asennus ilman kaapelointia.
- **Tyypilliset käyttökohteet:** Luukut, venttiilit, tekniset tilat, pumppaamot ja vedenottamot.

4.6.7 Tiedonkeruualustat tiedon koontiin ja tilannekuvan ylläpitoon

- Tiedonkeruualustojen päätavoitteet ja yleisimmät ominaisuudet:
    - Yhdistää hajautetut tiedot: Kerää automaattisesti eri turvajärjestelmien, sensoreiden ja laitteiden tuottaman datan yhteen hallintanäkymään – olipa kyse laajasta laitosalueesta tai useista fyysisesti erillisistä kohteista.
    - Älykäs ohjaus ja automaatio: Hyödyntää kerättyä dataa ohjatakseen järjestelmiä ja prosesseja automaattisesti, mikä parantaa reagointikykyä ja vähentää manuaalista työtä.

  - Reaaliaikainen valvonta: Monitoroi järjestelmien tilaa sekä operatiivisesti että teknisesti, mahdollistaen nopean häiriönhallinnan ja ennakoivan kunnossapidon.
  - Automaattinen rekisteröinti: Luo kattavan järjestelmä- ja laiteluettelon kaikista liitetyistä komponenteista, mikä helpottaa omaisuudenhallintaa ja vesihuoltolaitoksen sisäisiä auditointeja.
  - Tietoon perustuva päätöksenteko: Tarjoaa reaaliaikaisen BI-raportoinnin ja analytiikan, jotka tukevat strategista suunnittelua ja operatiivista optimointia.
- Huomiona, että palvelualustan käyttöönotto vaatii riittävät henkilöresurssit, jotta:
  - Alusta saadaan tavoitteen mukaisesti toimintaan
  - Data kerätään halutuista järjestelmistä ja oleelliset toiminnallisuudet tunnistetaan
  - Toimintaa voidaan tehostaa ja tilannekuvaa ylläpitää
- Tiedonkeruualustan käyttöönotto edellyttää toiminnan ymmärrystä ja suunnittelua, mutta panostus palkitsee myöhemmin reaaliaikaisella ja kattavalla tilannekuvatiedolla, joka tehostaa poikkeamien tunnistamista sekä tukee päätöksentekoa ja häiriötilanteiden hallintaa.

Tiivistetysti: Tiedonkeruualustat
- **Tarkoitus:** Kerää hajautetut tiedot yhteen näkymään, mahdollistaa älykkään ohjauksen ja tarjoaa reaaliaikaisen tilannekuvan päätöksenteon tueksi.
- **Mihin soveltuu:** Laajoihin laitosalueisiin ja hajautettuihin vesihuollon kohteisiin, joissa tarvitaan keskitetty hallinta ja nopea reagointi.
- **Käyttöönotto:** Vaatii riittävät resurssit, toiminnan ymmärrystä ja suunnittelua, mutta panostus palkitsee kattavalla tilannekuvalla ja tehostetulla häiriötilanteiden hallinnalla.

4.7 PALVELUT JA TOIMINTAMALLIT

Fyysisen turvallisuuden toteuttaminen ei perustu pelkästään teknisiin ja rakenteellisiin ratkaisuihin, vaan siihen liittyy myös erilaisia palveluita ja toimintamalleja, jotka tukevat kokonaisvaltaista suojausta. Palvelut, kuten vartiointi ja huolto, täydentävät rakenteellisia ja teknisiä keinoja ja varmistavat, että turvallisuus on jatkuvaa ja hallittua.

Pääasialliset palvelut vesihuollon ympäristössä

- **Etävalvonta ja hälytyskeskuspalvelut**
  - Kameravalvonta, kulunvalvonta ja hälytysjärjestelmät liitetään vartiointiliikkeen tai palveluntarjoajan valvomoon. Hälytyskeskus reagoi poikkeamiin ja ohjaa tarvittaessa toimenpiteitä, kuten hälyttää viranomaiset tai lähettää vartijan paikalle.
  - Soveltuu ympäristöön, jossa jatkuva fyysinen vartiointi ei ole kustannustehokasta.
  - Mahdollistaa nopean reagoinnin ilman paikallista henkilöstöä.
- **Teknisten järjestelmien ylläpito ja huoltopalvelut**
  - Fyysisen turvallisuuden ratkaisut, kuten lukitusjärjestelmät, kamerat ja hälytyslaitteet, vaativat säännöllistä huoltoa ja tarkastuksia. Palvelusopimukset varmistavat, että laitteet toimivat luotettavasti ja häiriöt korjataan nopeasti.
- **Kulunvalvontapalvelut ja avainhallinta**
  - Kulkuoikeuksien hallinta on olennainen osa fyysistä turvallisuutta. Palveluntarjoaja voi hoitaa avainten hallinnan, kulkuoikeuksien myöntämisen ja poistamisen sekä järjestelmien ylläpidon.

- **Hälytysjärjestelmien valvonta ja testaus**
  - Hälytysjärjestelmien toimivuus varmistetaan säännöllisillä testeillä ja valvonnalla. Tämä voidaan sisällyttää palvelusopimukseen.
- **Piirivartiointi**
  - Vartija kiertää useita kohteita ennalta sovitun aikataulun mukaisesti. Tämä voi olla perusteltua kohteissa, joissa on korostunut riski tai poikkeustilanne.
- **Paikallisvartiointi**
  - Vesilaitoksissa ei yleensä ole jatkuvaa paikallisvartiointia, mutta se voidaan järjestää tilapäisesti esimerkiksi suurissa häiriötilanteissa, korjaustöiden aikana tai kohteissa, joissa riskitaso on poikkeuksellisen korkea.

Kaikki edellä mainitut palvelut perustuvat sopimuksiin, joissa määritellään:

- Palvelun laajuus ja sisältö (esim. hälytyskeskuksen reagointiaika, huoltokäyntien tiheys)
- Vastuut ja velvoitteet (palveluntarjoaja vs. tilaaja)
- Raportointikäytännöt (hälytykset, poikkeamat, kuukausiraportit)
- Laatuvaatimukset ja auditointimenettelyt

Hyvin laadittu sopimus varmistaa, että palvelut tukevat kohteen riskienhallintaa ja täyttävät huoltovarmuuskriittisten kohteiden vaatimukset.

Tiivistetysti: Fyysisen turvallisuuden palvelut

- **Etävalvonta ja hälytyskeskuspalvelut:** Kameravalvonta, kulunvalvonta ja hälytysjärjestelmät liitetään valvomoon, joka reagoi poikkeamiin ja ohjaa toimenpiteitä.
- **Teknisten järjestelmien huolto:** Lukitus-, kamera- ja hälytysjärjestelmien säännöllinen huolto ja tarkastus varmistavat toimintavarmuuden.
- **Kulunvalvonta ja avainhallinta: Kulkutunnisteiden** hallinta ja kulkuoikeuksien ylläpito.
- **Vartiointipalvelut:** Piirivartiointi tai tilapäinen paikallisvartiointi riskiperusteisesti

Palvelusopimukset määrittävät laajuuden, vastuut ja laatukriteerit.

4.8 CPTED-MALLI – RIKOSTEN EHKÄISY YMPÄRISTÖN SUUNNITTELUN KEINOIN

CPTED-malli on tapa lähestyä rakennetun ympäristön suunnittelua rikoksien vähentämisen näkökulmasta. Lyhenne CPTED tulee sanoista Crime Prevention Through Environmental Design. Tästä käy ilmi mallin keskeinen ajatus siitä, että rikollisuuteen ja rikosten pelkoon voidaan vaikuttaa vähentävästi erilaisilla fyysisen ympäristön suunnittelun keinoilla. Ympäristöön ja rakennuksiin liittyvillä suunnitteluratkaisuilla pyritään vähentämään tai kokonaan poistamaan mahdollisuus rikoksen tapahtumiseen mahdollisuus. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

CPTED-malli koostuu viidestä periaatteesta:

1. Fyysinen turvallisuus
2. Liikkumisen kontrollointi
3. Tilojen huolto ja ylläpito
4. Puolustettava tila
5. Valvonta

CPTED-mallin erityispiirre on sosiaalisen ulottuvuuden huomioiminen. Tämä tarkoittaa esimerkiksi asuinalueiden kontekstissa tarkoittaa sitä, että alueella asuvan yhteisön jäsenet kokevat alueen omakseen ja suorittavat luonnollista valvontaa. Sillä, miten fyysinen ympäristö suunnitellaan, pyritään lisäämään tilan käyttäjien positiivista suhdetta tilaan ja lisäämään kokemusta tilan omistajuudesta. Kun tila koetaan omaksi, sitä todennäköisemmin puolustetaan. Käytännön esimerkki siitä, miten tämä periaate voi toteutua työkäyttöön tarkoitetuissa tiloissa on niiden huolto ja ylläpito. Alueen ja kohteiden aktiivinen kunnossapito antaa samalla ulospäin signaalin siitä, että kyseisestä alueesta/kohteesta pidetään huolta ja sitä valvontaan aktiivisesti. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

Puolustettavan tilan käsite onkin yksi CPTED-mallin keskeisistä periaatteista ja sillä tarkoitetaan sellaista ympäristöä, josta potentiaalinen rikoksentekijä voi tulkita, että tilan käyttäjät kontrolloivat aluettaan ja välittävät siitä. Valvotulla alueella rikoksen havaitsemisen ja kiinnijäämisen riski kasvaa ja tämä vähentää rikoksentekijän mielenkiintoa kohteeseen. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

Fyysisellä turvallisuudella tarkoitetaan käytännön keinoja, joilla yksittäisen kohde pyritään suojaamaan hyökkäykseltä ja/tai luvattomalta tunkeutumiselta. Esimerkkejä tällaisista keinoista ovat kulunvalvonta-, murtoilmaisu- ja kameravalvontajärjestelmät, lukitusjärjestelmät, aidat ja puomit sekä muut rakenteelliset suojausratkaisut. Fyysinen turvallisuus on syytä huomioida arkkitehtuurisilla ratkaisuilla tila- ja pihasuunnittelussa. Muun muassa kasvien ja kasvuston sekä erinäisten pihaelementtien sijoittelulla voidaan saada aikaan merkittäviäkin turvallisuusvaikutuksia, hyödyntäen niitä muun muassa eri alueiden ja kulkuteiden rajaamisessa, näköesteenä tai esteenä tunkeutumiselle. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

Liikkumisen kontrollointi tarkoittaa sitä, että kohteessa saa liikkua vain työperusteisin syin. Tähän liittyy kaikkien tiloissa liikkuvien luvittaminen, jotta voidaan selkeämmin erottaa joukkoon kuulumattomat. Luvittamisen tavoite on yksilöllistä tunnistamista lisäämällä vähentää pahantahtoisen henkilön mahdollisuuksia toimia anonyymisti. Tilaluokittelu on osa liikkumisen kontrollointia. Kun julkiset, puolijulkiset ja yksityiset tilat on selvästi eroteltu ja nimetty, on helpompaa määritellä millä perusteilla missäkin tilassa saa oleskella. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

Valvonta kytkeytyy kaikkiin muihin periaatteisiin ja sitä voidaan toteuttaa kolmessa eri muodossa. Kaikkien muotojen tavoite on muokata fyysistä ympäristöä, siten että se tarjoaa mahdollisimman vähän tilaisuuksia rikosten tekoon.

- Luonnollinen valvonta – Luonnollisella valvonnalla tarkoitetaan käyttäjien mahdollisuutta valvoa työskentelytilojaan osana arkipäiväänsä ja näin lisätä rikollisten kiinnijäämisen riskiä. Konkreettisia esimerkkejä ovat käyttäjän näkyvyyden lisäämisestä välittömään toimintaympäristöönsä ovat näkyvyyttä haittaavien esteiden poistaminen ja riittävästä valaistuksesta huolehtiminen.
- Organisoitu valvonta – Organisoidulla valvonnalla tarkoitetaan muodollista, ihmisen suorittamaa valvontaa (esim. vartiointi, poliisi).
- Mekaaninen valvonta – Mekaanisella valvonnalla tarkoitetaan fyysisiä suojauskeinoja, kuten valvontakameroita, lukitusta, murtoilmaisua, riittävää valaistusta jne. (Rikoksentorjuntaneuvosto 2025 A & B; Design for Security 2026.)

Vesilaitosympäristössä CPTED-mallia on mahdollista hyödyntää erityisesti uudiskohteita suunnitellessa, mutta myös vanhojen kohteiden fyysistä turvallisuuttaa kehittäessä. CPTED-näkökulmasta vesilaitos kaikkine yksittäisine kohteineen on puolustettavaa tilaa ja tilojen jokapäiväiset käyttäjät niitä, joilla on mahdollisuus suorittaa luonnollista valvontaa. Puolustettavan tilan käsite taas voidaan kytkeä henkilöstön sitouttami-

seen työnantajaansa ja *”olen vain töissä täällä”*-mentaliteetin vähentämiseen. Valvonnan eri muodot toteutuvat edellä kuvatun luonnollisen valvonnan lisäksi organisoidun eli vartioinnin suorittaman valvonnan sekä mekaanisilla ja fyysisillä keinoilla toteutetun valvonnan kautta. Liikkumisen kontrolli on keskeinen keino vesilaitosympäristön turvallisuuden toteuttamisessa.

Tiivistetysti: CPTED-malli

- Perustuu ajatukseen, että rikollisuutta voidaan vähentää fyysisen ympäristön suunnittelulla *(**C**rime **P**revention **T**hrough **E**nvironmental **D**esign)*.
- Tavoitteena on luoda ympäristö, joka lisää käyttäjien omistajuuden tunnetta ja luonnollista valvontaa, vähentää rikoksen mahdollisuuksia ja nostaa kiinnijäämisen riskiä.
- Käytännön keinoja toteutukseen, kuten rakenteelliset ratkaisut (aidat, lukitus), tekniset järjestelmät (kameravalvonta, kulunvalvonta), alue- ja pihasuunnittelu, hyvä valaistus ja selkeä tilaluokittelu.

4.9 JATKUVUUDEN VARMISTAMINEN NORMAALIOLOISSA

Tässä luvussa käsitellään organisaation toiminnan jatkuvuuden varmistamista fyysisen turvallisuuden viitekehyksessä normaalioloissa. Koska varautumisteemaa on käsitelty seikkaperäisemmin Vesihuoltopoolin julkaisussa *"Vesihuoltolaitosten opas häiriötilanteisiin varautumiseen”*, keskitytään tässä luvussa siihen, miten varautua häiriötilanteisiin fyysisen turvallisuuden keinoin. Varautumista poikkeusoloihin käsitellään luvussa 6.

Eri viranomaisten yhteistyönä tuottamassa oppaassa *”Häiriö- ja kriisitilanteisiin varautuminen”* määritellään erilaiset tilanteet seuraavasti:

- **Häiriötilanteella** tarkoitetaan esimerkiksi elintärkeiden toimintojen ja palveluiden katkoksia tai luonnonilmiön aiheuttamia tilanteita.
- **Kriisit** ovat tavanomaisia häiriöitä vakavampia tai pitkittyneitä tapahtumia.
- **Poikkeusoloilla** tarkoitetaan erittäin harvinaista ja vakavaa tilannetta, jonka hoitamiseen tarvitaan normaalista poikkeavia viranomaisvaltuuksia.

Tarkemmin määriteltynä poikkeusolojen syntyvät, kun valtioneuvosto yhteistoiminnassa tasavallan presidentin kanssa toteaa yhteiskunnan tilanteen sellaiseksi, että siihen kohdistuvia häiriöitä ei pystytä saamaan hallintaan normaalin lainsäädännön keinoin. Poikkeusoloissa otetaan käyttöön tavanomaisesta poikkeava lainsäädäntö, joka antaa lisää toimivaltuuksia viranomaisille. Häiriö- ja kriisitilanteet voivat tapahtua sekä normaali- että poikkeustilanteessa. Normaali- ja poikkeusolojen eroja on havainnollistettu kuvassa 19.

Toiminta tapahtuu normaaliolojen lainsäädännön puitteissa.	**TAVOITE** Toiminnan jatkuvuuden varmistaminen erilaisissa normaalitilanteen häiriö,- poikkeus- ja kriisitilanteissa, joiden **vaikutus on paikallinen.**	**OSALLISET** • Vesihuoltolaitos • Palveluntuottajat ja sidosryhmät • Viranomaiset
Toiminta tapahtuu tilanteessa, jossa valtionjohto on asettanut voimaan erityislakeja.	**TAVOITE** Toiminnan jatkuvuuden varmistaminen poikkeusoloissa, joilla on **laajempi alueellinen tai valtakunnallinen vaikutus.**	**OSALLISET** • Vesihuoltolaitos • Palveluntuottajat ja sidosryhmät • Viranomaiset * • Puolustusvoimat*

*** Poikkeustilanteessakin vastuu vesihuollon toiminnan turvaamisesta on aina lähtökohtaisesti vesihuoltolaitoksella itsellään!**
*** Vesihuoltolaitosten tulee varautua toimimaan myös tilanteissa, joissa viranomaisavun saamisessa on viivettä.**

Kuva 19 Normaaliolojen ja poikkeusolojen ero.

Yhteiskunnan turvallisuusstrategiassa todetaan, että yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat voivat johtua ihmisen toiminnasta, luonnonvoimista tai olla teknologisen kehityksen seurausta. Tarkempia tietoja organisaation varautumistarpeiden määrittelyn tueksi saa sisäisen turvallisuuden *TUOVI-portaalissa* julkaistuista alueellisista riskiarvioista. Alueellisissa riskiarvioissa on tunnistettu Suomen eri alueille ominaisia riskejä, jotka toteutuessaan aiheuttavat merkittäviä alueellisia vaikutuksia sekä arvion niiden todennäköisyydestä.

Kokonaisturvallisuuden sanaston määritelmän mukaan **jatkuvuudenhallinnalla** tarkoitetaan huoltovarmuutta parantavaa, jatkuvaa organisaation **prosessia**, jolla

1) tunnistetaan toimintaan kohdistuvat uhat ja
2) arvioidaan niiden vaikutuksia organisaatioon sekä sen toimijaverkostoon ja
3) luodaan toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle.

Jatkuvuudenhallinnan prosessilla siis luodaan toimintatavat vakavia häiriötilanteita varten siten, että toiminta voidaan turvata kaikissa olosuhteissa. Jatkuvuudenhallinnan prosessille ominaista on jatkuva kehittäminen sekä säännöllisesti ylläpidettävä toiminta, jossa otetaan huomioon oman toiminnan lisäksi yhteistyö- ja palvelukumppanien kyky toimia häiriötilanteissa.

Kokonaisturvallisuuden sanaston määritelmän mukaan **varautuminen** on **toimintaa**, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdolliset poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Valmius puolestaan on tila, joka on saavutettu varautumisella. (Sanastokeskus 2017).

Häiriötilanteisiin varautumisessa on tärkeää tehdä yhteistyötä viranomaisten, kunnan, materiaalitoimittajien, palveluntarjoajien, asiakkaiden ja muiden sidosryhmien kanssa. Vesilaitosyhdistyksellä on paljon materiaaleja, joissa on laajasti käsitelty jatkuvuuden hallintaa ja siihen liittyviä hyviä käytänteitä. Näihin on erikseen viitattu ***liitteessä 1***, johon on koostettu tämän oppaan sisällön kannalta oleellisia tukimateriaaleja.

Fyysisen turvallisuuden näkökulmasta jatkuvuudenhallinta ja varautuminen edellyttävät kriittisten kohteiden tunnistamista ja niiden suojaamisen suunnittelua, varautumista materiaalien ja kemikaalien saatavuuden varmistamiseen, tietoturvallisuuden hallintaa sekä teknisten järjestelmien toimintakyvyn varmistamista. Alla kuvataan keskeiset toimenpiteet ja parhaat käytännöt näihin liittyen.

Jatkuvuuden varmistamisen kannalta kriittisten kohteiden suojaaminen
Toimenpiteet ja esimerkit:

- Tunnista kriittiset sähkönkäyttökohteet, jotka tarvitaan:
    - talousveden tuotannossa ja jakelussa varmistamaan häiriön aikaista kulutusta vastaava vedentuotanto, vedensaanti yhteiskunnan toimivuuden kannalta kriittisille kohteille ja jakeluverkoston minimipaineen ylläpitoon hygieniariskin välttämiseksi tai
    - viemäröinnissä ja jätevedenpuhdistuksessa ympäristöterveyden ja ympäristönsuojelun kannalta keskeisimmät jätevedenpumppaamot ja lupaehtojen mukaisen toiminnan edellyttämä jätevedenkäsittely.
- Tunnista kriittiset materiaalit (kemikaalit, varaosat yms.)
- Suojaa varavoimajärjestelmät, muuntajat ja sähkönjakelupisteet lukituin tiloin, asianmukaisilla kulkuoikeuksilla ja murtoilmaisujärjestelmällä.
- Suojaa materiaalivarastot lukituin tiloin, asianmukaisilla kulkuoikeuksilla ja murtoilmaisujärjestelmällä.
- Varmista varavesisäiliöiden häiriöttömyys esimerkiksi kameravalvonnalla
- Toteuta kameravalvontaa kriittisten tilojen tai kohteiden valvonnassa ja varmista, että tallenteet säilyvät riittävän pitkään (esim. 30 vrk).
- Tee riskikartoitus ja priorisoi kohteet, joihin kohdistuu suurin sabotaasi- tai ilkivaltariskin uhka.

Varmuusvarastointi ja kemikaalien hallinta

- Ylläpidä varmuusvarastoa kriittisille kemikaaleille ja tarvikkeille.
- Harkitse, voitko varastoida sellaisia teknisiä laitteita, jotka ovat vanhentuneita mutta toimivia.
- Tee yhteistyösopimuksia lähialueen vesilaitosten kanssa varmistusjärjestelyistä, kuten materiaaliset ja toiminnalliset yhteistyöt.
- Varmista, että kemikaalien vastaanottoa valvoo oma henkilöstö ja että varastotilat ovat lukittuja sekä suojattu asianmukaisilla kulkuoikeuksilla ja murtoilmaisujärjestelmällä.

Sopimustekniset ja hallinnolliset toimenpiteet

- Tunnista vesihuoltolaitoksen kriittiset palvelut (perustoiminnan ylläpitämät palvelut, kuten logistiikka) ja varmista normaaliolojen aikana palveluiden riittävä saatavuus myös poikkeusolojen sattuessa hyödyntäen esimerkiksi VAP-varauksia tai SOPIVA-sopimuslausekkeita.
- Tarkasta ja ylläpidä kriittisten tilojen ja kohteiden kulkuoikeuksia siten, että vain oikeudellisilla henkilöillä on kulkuoikeudet.
- Varmista turvajärjestelmien ylläpito ja huolto sekä ennakoi turvajärjestelmien uudistaminen ennen elinkaaren päättymistä ja tietoturvapäivitysten loppumista.
- Huolehdi paloturvallisuusjärjestelmien olemassaolosta ja toimivuudesta
- Tee säännöllisesti tarkastus fyysisen turvallisuuden nykytilasta, kuten turvajärjestelmien päivitystarpeista tai fyysisten rakenteiden kunnosta.
- Tee säännöllisesti varavoimakoneiden käyttöönoton ja toimivuuden testaukset

Tiedonhallinta ja avoimet lähteet

- Vältä julkaisemasta arkaluontoista tietoa (esim. tarkkoja karttoja, kriittisiä laitepaikkoja, ID-korttien ulkoasuja) verkkosivuilla tai muissa avoimissa lähteissä.
- Tarkista säännöllisesti hakukoneilla ja tekoälytyökaluilla, ettei verkon avoimissa lähteissä ole laitosta koskevaa riskialtista tietoa.
- Laadi sisäinen ohjeistus siitä, mitä tietoa saa julkaista ja mitä ei.

Henkilöstön tietotaito ja poistuvat työntekijät

- Määritä jatkuvuuden kannalta kriittisiä tehtäviä hoitavat henkilöryhmät (oma ja palveluntarjoajien henkilöstö) ja huomioi tarvittavat oikeasuhtaiset toimenpiteet henkilöturvallisuuden varmistamiseksi (esim. perehdytys, pääsyoikeudet, turvallisuusosaaminen). Tunnistetut avainhenkilöt tulee olla nimetty ja heillä tulee olla tehtävään perehdytetyt varahenkilöt.
- Varmista avainten, karttojen ja dokumenttien palautus työsuhteen päättyessä.
- Sisällytä työsopimuksiin salassapitovelvoitteet tai käytä erillistä salassapitosopimusta.
- Rajoita karttatietojen jakelua urakoitsijoille vain välttämättömään.
- Käytä palautuslistaa ja tee tarkistus ennen työsuhteen päättymistä.

Ulkoistettujen palveluiden hallinta

- Aseta ulkoisille toimijoille samantasoiset turvallisuusvaatimukset kuin omalle henkilöstölle.
- Rajoita pääsy kriittisiin kohteisiin vain välttämättömään ja tarkasta pääsyoikeudet säännöllisesti.
- Sisällytä sopimuksiin turvallisuuslausekkeet ja toimittajien pätevyysvaatimukset.
- Tee taustaselvitys toimittajista ennen sopimuksen solmimista.

Tietotekniikan ja turvajärjestelmien suojaaminen

- Suojaa kaukovalvonta- ja käyttöjärjestelmät UPS-laitteistolla, joka mahdollistaa hallitun alasajon sähkökatkon aikana.
- Varmista myös kameravalvontajärjestelmien toiminta UPS-laitteilla.
- Kulunvalvonta- ja murtohälytysjärjestelmät tulee varmistaa varakäyntiakustoilla:
    - Kulunvalvontajärjestelmä: vähintään **2 tunnin** varakäyntiaika.
    - Murtohälytysjärjestelmä: vähintään **24 tunnin** varakäyntiaika.
- Tarkista UPS-laitteistojen ja varakäyntiakustojen kunto säännöllisesti.

Tiivistetysti: Jatkuvuuden varmistaminen, viitekehyksenä fyysinen turvallisuus

- Tunnista laitoksen toiminnan kannalta jatkuvuuden varmistamisen kriittiset kohteet sekä suojaa ne fyysisesti ja valvo soveltuvin turvajärjestelmin
- Varmista kemikaalien ja tarvikkeiden saatavuus varmuusvarastoinnilla ja yhteistyöllä muiden laitosten kanssa sekä suojaa nämä varmuusvarastot
- Hallitse sopimukset, kulkuoikeudet ja turvajärjestelmien elinkaari.
- Suojaa arkaluontoinen tieto ja tarkista avoimien lähteiden laitoskohtaiset tiedot.
- Huolehdi poistuvien työntekijöiden salassapitovelvoitteesta ja omaisuuden palautuksesta.
- Aseta ulkoisille toimijoille samat turvallisuusvaatimukset kuin omalle henkilöstölle.
- Määritä toiminnan kannalta kriittiset avainhenkilöt ja heidän varahenkilönsä.
- Varmista tietotekniikan ja turvajärjestelmien toiminta UPS-laitteilla ja varakäyntiakustoilla.

4.10 FYYSISET TUNKEUTUMISTESTAUKSET

Fyysiset tunkeutumistestaukset ovat keino luoda käsitys oman organisaation fyysisten suojauskeinojen nykytilasta ja toimivuudesta sekä organisaation turvallisuuskulttuurin tasosta. Fyysisessä tunkeutumistestauksessa asiakasorganisaation valtuuttama tunkeutuja pyrkii pääsemään asiakasorganisaation tiettyyn, ennalta määriteltyyn kohteeseen (esim. rakennus, tekninen tila).

Tunkeutumistestaus on rinnastettavissa mystery shopping-tutkimukseen, jossa asiakkaana esiintyvä tutkimuksen suorittaja havainnoi henkilökunnan toimintaa asiakaspalvelutilanteissa ja sitä, vastaako se asiakasorganisaation ohjeistusta ja tavoitetasoa. Fyysisessä tunkeutumistestauksessa periaate on sama, mutta havainnoinnin kohteena on fyysisten suojauskeinojen lisäksi henkilökunnan turvallisuustietoisuuden ja –osaamisen nykytila ja toteutuminen käytännössä.

Fyysinen tunkeutumistestaus pyrkii tuottamaan sen tilanneelle taholle ymmärryksen siitä, kuinka hyvin henkilökunta ja/tai kohteella toimivat sidosryhmät tuntevat turvallisuusohjeistuksen ja noudattavat sitä sekä miten henkilökunta tai kohteella toimivat sidosryhmät toimivat kohdatessaan vieraan henkilön toimitiloissa tai muulla organisaation hallinnassa olevalla alueella. Testaus myös luo käsityksen siitä, onko henkilökunnalla ja/tai kohteella toimivilla sidosryhmillä ymmärrys siitä, mitkä ovat oman organisaation kriittisiä tiloja ja keitä niihin saa/ei saa päästää.

Tiivistetysti: Fyysiset tunkeutumistestaukset

- Selvitä ulkopuolisella, riippumattomalla tunkeutumistestillä organisaatiosi fyysisen suojauksen nykytila ja turvallisuuskulttuurin taso sekä niiden mahdolliset haavoittuvuudet.
- Hyödynnä tunkeutumistestauksen tuloksia kehitystoimenpiteiden suunnittelussa.

5 FYYSISEN TURVALLISUUDEN ELINKAARI

5.1 ESISUUNNITTELUVAIHE – UUDIS- TAI SANEERAUS-KOHDE

Uudistusta tai saneerausta suunnitellessa tulee osallistaa toiminnan kannalta olennaiset sidosryhmät tuottamaan näkemyksiä koskien uudistustarpeita ja kriittisyyden määrittelyä. Näin saadaan eri käyttäjäryhmien näkemyksiä siitä, mikä uudis- tai saneerauskohteessa vaatii suojaamista tai suojaamiskeinojen päivitystä. Kriittisyyden turvaamisen keinot eivät välttämättä ole sidoksissa pelkästään fyysisen turvallisuuden suojauskeinoihin, vaan ne voivat liittyä esimerkiksi kriittisten toimintojen tai järjestelmien kahdennukseen taikka hallinnollisiin ohjeisiin. Sidosryhmät huomioimalla saadaan kokonaisvaltaisempi näkemys kustannustehokkaista keinoista toteuttaa toiminnan jatkuvuuden varmistaminen.

Riippumatta siitä onko esisuunnitteluvaiheessa kyse uudis- tai saneerauskohteesta, tulee tässä vaiheessa määrittää hankkeen kokonaistavoite (miksi toteutetaan, mitä halutaan saavuttaa) sekä toteuttaa kohteen riskienarviointi ja kriittisyyden arviointi, mitkä määrittävät myös fyysisen turvallisuuden suojauskeinojen suuntaviivat jo esisuunnitteluvaiheessa. Esisuunnitteluvaiheessa pyritään saamaan suuntaviivoja hankkeen kokonaiskustannuksiin vaikuttavista tekijöistä määritetyn tavoitteen mukaisesti.

”Liite 2 - Fyysisen turvallisuuden hinta-arviot” sisältää turvatekniikan, fyysisen turvallisuuden ja turvallisuuspalveluiden hinta-arvioita mm. budjetoinnin tueksi, kun vesihuoltolaitos suunnittelee fyysisen turvallisuuden kehittämistä esimerkiksi saneeraus- tai uudistamishankkeessa.

5.1.1 Uudisrakennushankkeen esisuunnitteluvaihe

- Riskienarviointi, mitä uhkia kohteeseen kohdistuu?
- Kriittisyyden arviointi, kohteessa toteutettavan toiminnan kriittisyys vesihuollon toimintaan?
- Ennakoidut käyttäjät ja käyttäjäryhmät sekä kohteen käyttöaste?
- Onko olemassa olevia turvajärjestelmiä, jotka olisivat tavoitteen mukaista laajentaa kohteeseen? Tämä määrittää jo osaltaan kohteeseen mahdollisesti valikoituvat järjestelmät.
- Uudisrakennushankkeen esisuunnitteluvaiheen viitekehys turvallisuuden näkökulmasta voi koostua mm.:
    - Kohteen fyysisen sijainnin valinnasta, esimerkiksi:
        - kohteen toteuttaminen maan alle vai maan päälle
        - kriittisten toimintojen sijoitus kauemmaksi tontin rajasta
        - muut ympäristöön liittyvät tekijät ja näiden mahdolliset maanrakennustarpeet.
    - Ennakoidut tekniset turvajärjestelmävaatimukset
    - Ennakoidut rakenteellisen turvallisuuden vaatimukset

5.1.2 Saneeraushankkeen esisuunnitteluvaihe

- Riskienarviointi, mitä uhkia kohteeseen kohdistuu?
- Kriittisyyden arviointi, kohteessa toteutettavan toiminnan kriittisyys vesihuollon toimintaan?
- Fyysisen turvallisuuden nykytilan arviointi:

    - Nykyisten järjestelmien kunto, elinkaari ja puutteet sekä kaapelointien kunto ja toteutustapa?
    - Mikä on turvatekniikan järjestelmien dokumentaation taso?
    - Miten avainhallinta on hoidettu? Onko mahdollista, että avaimia on hävinnyt?
- Turvajärjestelmien laadukkaan saneeraussuunnittelun perusta on kattava ja ajantasainen dokumentaatio. Jos dokumentaatiota ei ole tai se on vanhentunutta, on esisuunnitteluvaiheessa käytettävä enemmän aikaa nykytilan selvittämiseen. Jos nykytilaa ei selvitetä tarkemmin, on hyväksyttävä, että mahdollisen saneerauksen kustannusarvio on huomattavasti epätarkempi. Viimeistään perussuunnitteluvaiheessa on suositeltavaa, että nykytila todetaan tarkasti tarkempien suunnitelmien toteuttamiseksi.
- Saneeraushankkeen esisuunnitteluvaiheen viitekehys turvallisuuden näkökulmasta voi koostua mm.:
    - Teknisten turvajärjestelmien uudistamis- tai laajennustarpeiden määrittämisestä
    - Rakenteellisen turvallisuuden uudistamis- tai laajennustarpeiden määrittämisestä

5.2 PERUSSUUNNITTELUVAIHE

Vesilaitoshankkeen onnistumisen perustana on se, että strategiset tavoitteet sekä vähimmäisvaatimukset määritellään selkeästi heti alussa. Tämä varmistaa, että kaikilla osapuolilla on yhteinen ymmärrys hankkeen suunnasta sekä siitä, mitä tulee saavuttaa. Perussuunnitteluvaiheessa luodaan hanketta varten urakkalaskenta- ja toteutussuunnitelmat, joiden avulla kokonaisuus on mahdollista hankkia ja toteuttaa.

Tätä opasta voidaan hyödyntää osana perussuunnitteluvaihetta ja se toimii tukena turvallisuusasioista vastaaville. Opas tukee päälliköiden, työnjohdon, projektipäälliköiden, rakennuttajien, suunnittelijoiden sekä turvallisuudesta vastaavien työtä. Se auttaa niin saneeraus- kuin uudiskohteissa fyysisen turvallisuuden parantamisessa ja tarjoaa konkreettisia työkaluja turvallisuuden kehittämiseen. Opas auttaa arvioimaan, ollaanko menossa oikeaan suuntaan, tunnistamaan kehityskohteet sekä mahdollisuudet, ja antaa eväitä perustella turvallisuusrakenteiden tarpeellisuutta rahoittajille.

- Päätös uuden laitoksen rakentamishankkeen tai saneeraushankkeen edistämisestä perussuunnitteluvaiheeseen, kun esisuunnitteluvaiheesta on saatu oleelliset tiedot päätöksenteon tueksi, kuten alustavat kustannusarviot hankkeesta.
- Toteutukseen osallistuvat nimetään:
    - Johto määrittää strategiset tavoitteet vesihuoltokohteelle
    - Hankevastaavat vastaavat tavoitteiden konkretisoinnista sekä oppaan linjausten huomioimisesta.
    - Suunnittelijat laativat urakkalaskenta- ja toteutussuunnitelmat, joissa huomioidaan ajantasainen teknologia ja tulevaisuuden tarpeet.
    - Huomioitavaa: Vastuuroolit ja -rajat kirjataan selkeästi vastuurajataulukoihin (esim. kuka vastaa mistäkin osa-alueesta).
- Teknisiä suosituksia ja vaatimuksia kirjataan hankintoja varten, huomioiden tekniikan kehitys (esim. onko ratkaisu vielä relevantti kahden vuoden päästä).

5.2.1 Vastuut ja rajapinnat sekä resurssit ja osaaminen

Jokaisessa hankkeen vaiheessa vastuut sekä eri toimijoiden rajapinnat tulee dokumentoida huolellisesti, esimerkiksi vastuurajataulukoiden avulla. Näin vältetään epäselvyydet ja varmistetaan sujuva yhteistyö urakoitsijoiden, suunnittelijoiden ja käyttöhenkilöstön kesken.

Resurssien ja osaamisen riittävyys on tärkeää: toimintaa ei saa rakentaa yhden henkilön varaan. Vaikka osa palveluista ulkoistettaisiin, tulee varmistaa, että organisaatiossa säilyy riittävä turvallisuuden ja tekniikan osaaminen. Fyysisen turvallisuuden lisääminen ja valvontatekniikan käyttöönotto tuovat lisätyötä, eikä valvonta voi olla pelkästään ulkoistettu – kriisitilanteessa palvelua ei välttämättä saada riittävästi ulkopuolisilta tuottajilta. Vesilaitoksella on oltava omaa osaamista tiedon hyödyntämiseen ja nopeaan reagointiin.

5.2.2 Teknologian kehityksen huomioiminen

Hankinnoissa ja suunnittelussa on tärkeää ottaa huomioon ratkaisujen elinkaari ja tulevaisuuden yhteensopivuus. Tekniikan jatkuva kehittyminen edellyttää, että valitut järjestelmät ovat päivitettävissä ja tukevat laitoksen toimintaa pitkällä aikavälillä.

Oikein hyödynnettynä moderni teknologia ja automaatio voivat tehostaa toimintaa ja mahdollistaa resurssien kohdentamisen järkevämmin – joskus jopa vähentää henkilöresurssien tarvetta. Esimerkiksi analytiikkatoiminnot pystyvät tunnistamaan poikkeamia, joihin voidaan reagoida nopeasti. Tämä vaatii kuitenkin järjestelmien alkuinvestointeja sekä ylläpitokustannukset tulee ottaa huomioon.

5.2.3 Resurssien kohdentaminen ja minimitason varmistaminen

Alla on tarkistuslista, johon on koottu perussuunnitteluvaiheen keskeiset huomioitavat asiat. Tarkoitus on varmistaa, että tärkeimmät tehtävät tulevat suoritetuiksi järjestelmällisesti. Tämän avulla toimintatavat yhtenäistyvät ja riskit unohduksille minimoidaan. Listan avulla voidaan varmistaa eri näkökulmien huomioiminen perussuunnitteluvaiheen edetessä.

Tarvekartoitus ja riskianalyysi

- Onko tehty kattava riskianalyysi kohteesta?
- Onko nykyiset järjestelmät arvioitu (kunto, elinkaari, puutteet)?
- Onko määritelty turvallisuustason vaatimukset ja käyttäjien tarpeet?

Hankintamalli ja urakkamuoto

- Onko urakkarajat ja vastuut määritelty selkeästi?
- Onko hankinta-asiakirjojen tietoturvaluokat määritetty (mitä aineistoa julkaistaan osana kilpailutusta, mitä toimitetaan vasta esimerkiksi urakkasopimusneuvotteluissa?)
- Onko kilpailutukseen määritetty soveltuvat laatu- ja hintapisteytysmallit?

Tekninen määrittely

- Onko määritelty tarvittavat laitteet ja näiden tekniset vähimmäisvaatimukset (mm. lukijat, ohjaimet, palvelimet)?

- Onko määritelty oleelliset sijoituspisteet turvatekniikan laitteistolle, jolla ohjataan kulkua tai valvotaan tavoitteiden mukaisesti kohteiden turvallisuutta?
- Onko huomioitu teknisiä järjestelmiä tai sovelluksia määritettäessä, että ne **eivät olisi** ainoastaan yksittäiseen laitetoimittajaan sidottuja (”vendor lock”).
- Onko ohjelmistot ja käyttöliittymät valittu (esim. web-käyttöliittymä, mobiili-käyttöliittymä)?
- Onko järjestelmien integrointimahdollisuudet huomioitu (esim. kiinteistöautomaatio)?
- Onko kaikki tekniset ja toiminnalliset vaatimukset dokumentoitu?
- Onko käyttöönottosuunnitelma laadittu tai sisällytetty osaksi toimittajalle / urakoitsijalle osoitettavia toteutuksen vaatimuksia?

Tietoturva ja verkkoarkkitehtuuri

- Onko järjestelmät suunniteltu eriytettyyn turvaverkkoon?
- Onko tietoturvavaatimukset dokumentoitu ja hyväksytty sekä vaatimukset osoitettu myös toimittajille / urakoitsijoille?

Ylläpito ja elinkaaren hallinta

- Onko huolto- ja ylläpitosopimukset sisällytetty hankintaan?
- Onko varaosien saatavuus ja tuotetuki varmistettu?
- Onko järjestelmät sisällytetty PTS-suunnitelmaan?

Budjetointi ja aikataulutus

- Onko budjetti hyväksytty ja kohdekohtaisesti jaoteltu?
- Onko aikataulu realistinen ja yhteensopiva muun toteutuksen kanssa?

Koulutus ja käyttöönotto

- Onko käyttäjille suunniteltu koulutus sisällytetty osaksi toimittajalle osoitettavia toteutuksen vaatimuksia?
- Onko testaus ja koekäyttö aikataulutettu sekä tähän resursoitu vesihuoltolaitoksen omaa henkilöstöä?

5.3 HANKINTAVAIHE JA TIETOTURVA HANKINNASSA

5.3.1 Hankintavaiheen vähimmäisvaatimuksia

Turvatekniikan hankinta on kriittinen vaihe fyysisen turvallisuuden kokonaisuudessa. Sen onnistuminen vaikuttaa suoraan järjestelmien toimivuuteen, kustannuksiin ja siihen, kuinka hyvin ne tukevat organisaation turvallisuustavoitteita. Hankintavaiheessa tehtävät ratkaisut määrittävät pitkälti koko järjestelmän elinkaaren hallinnan, joten huolellinen valmistelu on välttämätöntä.

- Selkeiden teknisten ja toiminnallisten vaatimusten määrittely on perusta vertailukelpoisille tarjouksille.
    - Kun vaatimukset ovat yksiselitteisiä, tarjoajien ratkaisuja voidaan arvioida samoilla kriteereillä, mikä vähentää tulkinnanvaraa ja varmistaa, että lopputulos vastaa asetettuja tavoitteita.
    - Ilman tarkkoja vaatimuksia hankittava järjestelmä voi jäädä puutteelliseksi tai sisältää ominaisuuksia, jotka eivät palvele todellisia tarpeita.

    - Järjestelmähankintojen tulee sisältää mm. ohjelmistot, lisenssit, asennukset, konfiguroinnit ja dokumentaatiot sekä tarvittavat takuu-, huolto- ja ylläpitotyöt.
- Vastuurajojen määrittely on tärkeää.
    - Urakka- ja vastuurajataulukot selkeyttävät, kuka vastaa asennuksesta, ohjelmistojen konfiguroinnista, dokumentaatiosta ja ylläpidosta. Tämä ehkäisee epäselvyyksiä ja riitatilanteita projektin aikana.
    - Samoin aikataulujen sopiminen jo hankintavaiheessa luo ennakoitavuutta ja vähentää viivästysriskiä, mikä on olennaista kustannusten hallinnan kannalta.
- Sopimusehdot muodostavat hankinnan juridisen perustan
    - Ne turvaavat molempien osapuolten oikeudet ja velvollisuudet, käsittelevät muutosten hallintaa, salassapitoa ja laadunvarmistusta. Hyvin laaditut sopimusehdot tukevat projektin läpivientiä ja riskienhallintaa.
- Hankinnassa on huomioitava järjestelmien elinkaari:
    - Ylläpito, huolto ja varaosien saatavuus sekä ohjelmisto- ja tietoturvapäivitykset. Näin vältetään piilokustannukset ja varmistetaan, että järjestelmä pysyy toimintakykyisenä ja turvallisena pitkällä aikavälillä.
    - Hankinnoissa tulee määrittää palvelun tai järjestelmän toimintaa koskevat vähimmäisvaatimukset koko elinkaaren ajalle.
        - Palvelutasovaatimuksissa tulee huomioida esimerkiksi:
            - käytettävyys (availability)
            - vasteajat ja korjausajat (SLA)
            - huolto- ja ylläpitovaatimukset
        - Järjestelmien osalta tulee huomioida:
            - elinkaarituki (End of Life -tilanteet)
            - ohjelmistopäivitysten ja tietoturvapäivitysten saatavuus
- Tietojärjestelmät, tietoliikenneyhteydet ja tiedonhallinta
    - Mikäli hankinta sisältää tietojärjestelmiä, tietoliikenneratkaisuja tai tiedon käsittelyä, tulee näihin liittyvät vaatimukset määritellä erikseen.
        - Toimittajan tulee kuvata:
            - järjestelmän arkkitehtuuri ja riippuvuudet
            - käytettävät tietoliikenneyhteydet ja niiden suojaus
        - Tietojen osalta tulee määrittää:
            - tiedon omistajuus (kuuluu vesihuoltolaitokselle)
            - tiedon säilytys ja varmistaminen
            - lokitietojen tuottaminen ja säilytys
    - Järjestelmien tulee tukea organisaation tietoturva- ja pääsynhallintaperiaatteita
    - Ulkoistettujen palvelujen osalta tulee varmistaa, että tiedon sijainti ja käsittely täyttävät lainsäädännölliset vaatimukset
- Turvallisuusvaatimukset hankinnoille ja toimittajille:
    - Turvatekniikkaan, palveluihin sekä muihin fyysisen turvallisuuden kannalta kriittisiin hankintoihin tulee sisällyttää selkeät turvallisuusvaatimukset. Vaatimusten tavoitteena on varmistaa, että hankittavat ratkaisut tukevat vesihuoltolaitoksen toiminnan jatkuvuutta, häiriönsietokykyä ja tietoturvaa koko elinkaaren ajan. Turvallisuusvaatimukset tulee määritellä osana hankinnan valmistelua ja sisällyttää tarjouspyyntöihin, sopimuksiin sekä palvelukuvauksiin.
    - Turvallisuusvaatimusten määrittelyssä keskeistä on riskiperusteisuus: vaatimukset mitoitetaan kohteen kriittisyyden, toiminnan merkityksen ja tunnistettujen riskien perusteella.

- Toimitus- ja toimintavarmuuden varmistaminen
    - Toimittajalta tulee edellyttää kykyä tuottaa palvelu tai järjestelmä sovitulla palvelutasolla kaikissa tilanteissa, mukaan lukien häiriötilanteet ja poikkeusolot.
    - Toimittajan tulee tunnistaa ja kuvata palveluun liittyvät:
        - kriittiset riippuvuudet (esim. alihankkijat, tietoliikenneyhteydet, sähkönsaanti)
        - keskeiset haavoittuvuudet ja niiden hallintakeinot
    - Toimittajalla tulee olla dokumentoitu riskienhallinta- ja jatkuvuudenhallintamalli, joka kattaa myös häiriötilanteisiin varautumisen
    - Toimittajan tulee kyetä osoittamaan palvelun jatkuvuuden turvaavat varmistusratkaisut (esim. varajärjestelmät, redundanssi, varavoima)
- Auditointi- ja testausoikeudet
    - Vesihuoltolaitoksella tulee olla oikeus varmistaa toimittajan toiminnan vaatimustenmukaisuus.
    - Sopimuksiin tulee sisällyttää:
        - oikeus auditoida toimittajan toimintaa
        - oikeus testata palvelun tai järjestelmän toimivuutta
    - Testaus voi sisältää esimerkiksi:
        - järjestelmien toiminnallisuuden varmistamisen
        - fyysisen turvallisuuden järjestelyjen testaamisen
        - Toimittajan tulee korjata havaitut puutteet sovitun aikataulun mukaisesti

Huolellinen hankintavaihe ei ole pelkkä muodollisuus, vaan se on investointi järjestelmän toimivuuteen, turvallisuuteen ja kustannustehokkuuteen. Kun vaatimukset, vastuut, aikataulut ja sopimusehdot määritellään selkeästi, lopputulos on vertailukelpoinen, tavoitteiden mukainen ja hallittavissa koko elinkaaren ajan.

5.3.2 Tietoturvallisuus hankinnan aikana

Turvatekniikan hankintaan liittyvä tarjouskilpailu sisältää usein luottamuksellista tietoa, kuten teknisiä piirustuksia, järjestelmäarkkitehtuureja, turvallisuuteen liittyviä ratkaisuja sekä vesihuoltolaitoksen rakenteeseen liittyviä tietoja. Näiden tietojen suojaaminen on kriittistä sekä kilpailutuksen aikana, että sen päätyttyä.

Alla on kuvattu huomioitavia periaatteita, kun fyysisen turvallisuuden toimenpiteitä (kuten turvajärjestelmiä) kilpailutetaan uudis- tai saneeraushankkeessa.

Tietoturva hankinnassa:

- Ennen kilpailutuksen käynnistymistä on määritettävä tarkkaan, mitkä tarjouspyyntöasiakirjat ovat tietoturvan näkökulmasta tarjoajille julkaistavia ja mitkä toimitetaan kilpailutuksessa vasta myöhemmin.
    - Mitä tietoa voidaan jakaa tarjouspyyntömateriaalissa ja mitä tulee suojata?
- Tietoturvatoimenpiteitä:
    - Potentiaalisia tarjoajia pyydetään ilmoittautumaan osaksi kilpailutusta, eli tarjouspyyntöasiakirjat jaetaan vain niille, ketkä ilmoittavat mahdollisuudestaan osallistua tarjouskilpaan
    - Ennen tarjouspyyntökilpailuun osallistumista voidaan tarjoaja velvoittaa allekirjoittamaan vesihuoltolaitoksen laatima salassapitositoumus (NDA), joka koskee tarjouskilpailun aikana saatuja tietoja. Tämä NDA kattaa materiaalien

käsittelyn ja velvoittaa tarjoajan huolehtimaan siitä, ettei luottamuksellista aineistoa jää hallintaan ilman vesihuoltolaitoksen lupaa.
    - Tällä varmistetaan, että kilpailutuksen päätyttyä tarjoajilla ei ole oikeutta säilyttää piirustuksia, teknisiä liitteitä tai muuta aineistoa, joka voisi vaarantaa vesihuoltolaitoksen turvallisuuden tai liikesalaisuudet.
    - Käytännössä tämä tarkoittaa joko digitaalisen aineiston poistamista tai fyysisten dokumenttien tuhoamista vesihuoltolaitoksen ohjeiden mukaisesti.
    - Tarjoajan tulee sitoutua:
        - salassapitoon (esim. salassapitosopimus)
        - tietojen käsittelyyn ainoastaan sovittuun käyttötarkoitukseen ja pääsy tietoihin tulee rajata vain niille henkilöille, joilla on työtehtävän perusteella oikeus siihen
- Julkaistavat tarjouspyyntömateriaalit ovat tuotettu siten, että tarjoajan on mahdollista tuottaa niistä vertailukelpoinen tarjous urakan toteuttamisesta.
    - Tarjouspyyntömateriaalissa on yksiselitteisesti esitetty mm. hankittavan järjestelmän laajuus (esim. kappalemäärät) ja periaatekaavio (toimintaperiaate ja sidonnaisuudet muihin järjestelmiin tai kohteisiin)
    - Julkaistavien tarjouspyyntömateriaalien osalta on suositeltavaa, ettei kohteeseen tai laitokseen liittyviä **laitesijoituspiirustuksia tai aluesuunnitelmia** jaeta vielä kilpailutuksen esivaiheessa, kunhan muu julkaistava tarjouspyyntömateriaali on tuotettu siten, että se on yksiselitteinen. Kyseiset tarkentavat suunnitelmat voidaan jakaa potentiaalisille tarjoajille, kun ns. esikarsinta on tehty ja päätetty kenen toimijoiden kanssa edetään tarjousneuvotteluihin.
        - Huom! Valituissa menettelyissä on huomioitava etenkin hankintalainsäädännön vaatimukset ja velvoitteet, jotta tarjoajien yhdenvertaisuus voidaan varmistaa kilpailutuksen aikana.
- Valtiovarainministeriö on tuottanut oppaan *"Suositus tietoturvallisuudesta hankinnoissa"*, jota voi myös soveltaa osana hankintoja ja niiden tietoturvavaatimuksia.

5.4 TOTEUTUS- JA URAKOINTIVAIHE

Rakentamisen ja urakoinnin aikana fyysisen turvallisuuden toteutuminen on yhtä tärkeää kuin valmiissa kohteessa. Toteutusvaiheessa käsitellään luottamuksellisia asiakirjoja ja suunnitelmia, liikutaan kriittisillä alueilla ja tehdään asennuksia, jotka vaikuttavat suoraan kohteen turvallisuustasoon. Siksi tietoturvallinen asiakirjahallinta, urakka-alueiden hallinta ja laadunvarmistus ovat keskeisiä.

- Tietoturvallinen asiakirjahallinta tarkoittaa, että kaikki suunnitelmat, piirustukset ja dokumentit luokitellaan ja säilytetään hallitusti. Urakoitsijan on huolehdittava siitä, että työn aikaiset piirustukset ja järjestelmätiedot käsitellään tilaajan ohjeiden mukaisesti ja että ne palautetaan tai hävitetään asianmukaisesti projektin päätyttyä. Projektipankin käyttö ja selkeät ohjeet asiakirjojen luokittelusta ja säilytyksestä vähentävät tietovuotoriskiä.
- Urakka-alueen rajaus ja kulunhallinta ovat välttämättömiä luvattoman pääsyn estämiseksi. Työmaa-alueet tulee rajata selkeästi ja varmistaa, että niihin pääsevät vain asianmukaisesti tunnistetut ja oikeutetut henkilöt. Käytännössä tämä tarkoittaa lukittuja tai kulunvalvottuja alueita, joissa henkilöstön pääsy perustuu rooliin ja tarpeeseen. Näin estetään sekä tahattomat että tahalliset turvallisuusriskit.

- Laadunvarmistus ja urakan valvonta toteutuksen aikana on olennainen osa turvallisuuden varmistamista. Työn etenemistä tulee seurata säännöllisesti, jotta asennukset vastaavat suunnitelmia ja hyviä asennustapoja. Myös urakoitsija on syytä velvoittaa raportoimaan työmaan etenemisestä säännöllisesti.
- Rakentamisen aikana on huolehdittava siitä, että urakoitavat alueet pysyvät hallinnassa koko projektin ajan. Tämä sisältää selkeät vastuurajat, tiedottamisen urakan aikana ja sen varmistamisen, että kaikki työt tehdään sovittujen turvallisuusvaatimusten mukaisesti. Lisäksi on huomioitava, että vesihuoltolaitoksen henkilöstö saa riittävän koulutuksen järjestelmien käyttöön ja hallintaan, mikä tukee niiden tehokasta hyödyntämistä.

Toteutus- ja urakointivaiheen hallinta ei ole pelkkä tekninen prosessi, vaan osa kokonaisvaltaista riskienhallintaa. Kun asiakirjat, alueet ja työvaiheet hallitaan tietoturvallisesti ja fyysisesti suojatusti, varmistetaan, että kohde säilyy turvallisena myös rakentamisen aikana ja että lopputulos täyttää kaikki asetetut vaatimukset.

Toteutus- ja urakointivaiheen tarkastuslista:

- Asiakirja- ja suunnitelmahallinta
  - Varmista, että kaikki piirustukset ja dokumentit on luokiteltu ja tallennettu projektipankkiin.
  - Tarkista, että urakoitsijat noudattavat salassapitosopimusta ja tietoturvaohjeita.
  - Huolehdi, että vanhentuneet versiot poistetaan ja lopulliset dokumentit arkistoidaan.
- Urakka-alueen rajaus ja kulunhallinta
  - Toteuta selkeät rajaukset työmaa-alueille (aidat, lukitut ovet).
  - Käytä kulunvalvontaa tai henkilökortteja, jotta alueelle pääsevät vain oikeutetut henkilöt.
  - Tarkista, että vierailijat kirjataan ja valvotaan.
- Fyysinen suojaus rakentamisen aikana
  - Varmista, että kriittiset tilat (esim. tekniset huoneet) ovat lukittuja myös työn aikana.
  - Toteuta väliaikaiset suojaukset, jos pysyvät rakenteet eivät ole vielä valmiit.
- Laadunvarmistus ja dokumentointi
  - Suorita säännölliset tarkastukset työn etenemisestä ja asennusten laadusta.
  - Varmista, että toteutus vastaa hyväksyttyjä suunnitelmia ja hyviä asennustapoja.
- Henkilöstön hallinta ja ohjeistus
  - Tarkista, että urakoitsijoiden henkilöstö on perehdytetty turvallisuusohjeisiin.
  - Varmista, että käyttöönottokoulutus on aikataulutettu ennen järjestelmän luovutusta ja siihen on kiinnitetyt vesihuoltolaitoksen asianmukaiset henkilöt.
- Riskienhallinta ja tiedottaminen
  - Arvioi ja päivitä riskejä urakointivaiheen aikana.
  - Tiedota muutoksista ja aikatauluista kaikille osapuolille selkeästi.

5.5 KÄYTTÖÖNOTTO JA KÄYTÖN AIKAINEN TOIMINTA

Turvajärjestelmien, kuten kameravalvonta-, kulunvalvonta- ja murtohälytysjärjestelmien, käyttöönotto ja niiden oikea käyttö ovat keskeisiä fyysisen turvallisuuden varmistamisessa. Käyttöönoton yhteydessä on varmistettava, että:

- Järjestelmät on asennettu ja testattu urakkasopimuksen mukaisesti.
- Käyttäjät saavat riittävän koulutuksen järjestelmien käyttöön ja hallintaan.

- Dokumentaatio (käyttöohjeet, huolto-ohjeet, järjestelmäkaaviot) on toimitettu ja tallennettu asianmukaisesti.
- Hallinnolliset linjaukset ja ohjeistukset otetaan käyttöön: Näihin sisältyvät mm. käyttöoikeuksien hallinta, hälytyksiin reagointiprosessit ja tietoturvakäytännöt.
- Vastuurajataulukot päivitetään käyttö- ja ylläpitovaiheeseen sopiviksi, jotta on selkeästi määritelty, kuka vastaa järjestelmien käytöstä, huollosta, hälytyksiin reagoinnista ja dokumentoinnista.

5.5.1 Käytön aikainen hallinta

Järjestelmien toimivuuden varmistaminen ei pääty käyttöönottoon. Käytön aikainen hallinta sisältää:

- Toiminnan seuranta, kuten järjestelmien lokitietojen ja hälytyshistorian tarkastaminen säännöllisesti.
- Käyttöoikeuksien hallinta: Kulunvalvontajärjestelmissä käyttäjäprofiilien ja pääsyoikeuksien ajantasaisuus on kriittistä.
- Tietoturva: Ohjelmistopäivitykset ja salasanakäytännöt on pidettävä ajan tasalla.
- Hallinnolliset ohjeet: Hälytyksiin reagointia, vikailmoitusten käsittelyä ja raportointia koskevat ohjeet on oltava selkeästi määritelty ja jalkautettu.

Turvajärjestelmien hälytystiedot voidaan koota keskitettyyn tiedonkoontialustaan, joka yhdistää eri järjestelmien hälytykset yhteen näkymään. Tämän ratkaisun tavoitteena on:

- Tehostaa tiedon ymmärtämistä ja tulkintaa: Käyttäjä näkee kokonaiskuvan ilman, että tietoa tarvitsee hakea erillisistä järjestelmistä.
- Poikkeamien havaitseminen: Keskitetty analytiikka ja hälytyskorostukset auttavat tunnistamaan poikkeavat tapahtumat nopeammin.
- Raportointi ja dokumentointi: Alusta voi tuottaa automaattisia raportteja hälytyksistä ja toimenpiteistä.

Tiedonkoontialusta on erityisen suositeltava laajoissa vesihuoltokohteissa, joissa:

- Kohteita on maantieteellisesti hajautuneesti.
- Turvajärjestelmiä on useita ja niiden hallinta erikseen olisi tehotonta.
- Hälytysten nopea tulkinta on kriittistä toiminnan jatkuvuuden kannalta ja kohteiden tilan seurannan osalta.

5.5.2 Takuuaika ja huoltovelvoitteet

Urakkasopimukseen tulee kirjata järjestelmien takuuaika, joka on tyypillisesti kaksi vuotta. Takuuaikana:

- Toimittaja vastaa takuuhuolloista mahdollisissa vikatilanteissa.
- Vasteaika korjaustoimenpiteille määritellään sopimuksessa (esim. 24–72 tuntia kriittisille vioille).

Takuun päätyttyä on suositeltavaa sopia vähintään vuosittaisesta huolto- ja ylläpitotarkastuksesta, jonka suorittaa järjestelmän osaava toimittaja. Toimittajan vastuulla olevan huollon tulee olla suunnitelmallista ja dokumentoitua. Tarkastuksessa:

- Varmistetaan järjestelmän yleiskunto.
- Tunnistetaan korjaustarpeet ja päivitystarpeet.
- Dokumentoidaan tehdyt toimenpiteet ja mahdolliset kehitysehdotukset.
- Vastuurajataulukot päivitetään myös huoltosopimusten osalta, jotta vastuut ovat selkeät koko elinkaaren ajan.

5.6 PTS-SUUNNITTELU JA OMAISUUDENHALLINTASUUNNITELMA

Pitkän tähtäimen suunnitelma on strateginen roadmap, joka ohjaa organisaation kehittymistä ja fyysisen turvallisuuden näkökulmasta turvajärjestelmien hallintaa tulevaisuudessa (5–20 vuotta). Se varmistaa investointien ja resurssien oikea-aikaisen kohdistamisen sekä edistää järjestelmien jatkuvuutta. Lisäksi ennakoiva riskien tunnistamisen ja varautuminen mahdollistuu huomioiden lainsäädännön, teknologian ja ympäristön muutokset.

Uusi vesihuoltolaki edellyttää vesihuoltolaitoksilta omaisuudenhallintasuunnitelman laatimista. Tähän kuuluu olennaisena osana myös turvajärjestelmien hyödyntäminen kriittisen infrastruktuurin hallinnassa. ***Vesihuoltolaitoksen omaisuudenhallinnan käsikirja*** korostaa, että omaisuudenhallinta on systemaattinen prosessi suunnittelusta luopumiseen, ja sen tulisi kattaa vähintään 10 vuoden toimenpide- sekä taloussuunnitelma.

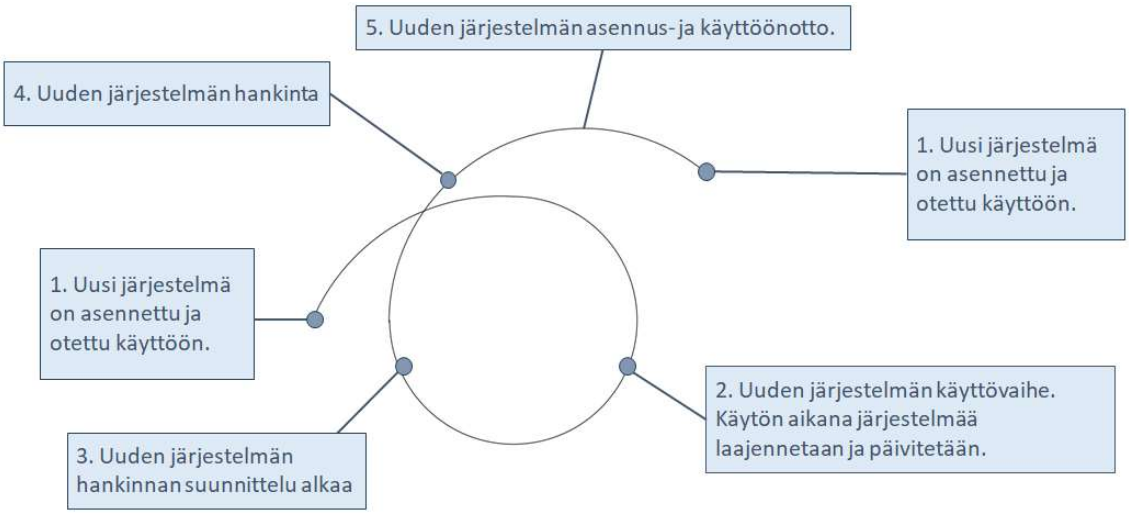
5.6.1 Turvatekniikan elinkaari

Turvatekniikan järjestelmien elinkaareen vaikuttaa seuraavat asiat, kuten:

- Patenttisuojauksen voimassaolo
  - Mekaanisten lukitusjärjestelmien patenttisuoja määrittää, kuinka kauan avaimia voi valmistaa vain valtuutetun valmistajan kautta. Patenttisuojan päättyminen lisää riskiä luvattomista kopioista ja voi edellyttää lukoston uusimista.
- End of Life (EOL) -ajankohdat
  - Ohjelmisto- ja laiteohjelmistopäivitykset loppuvat, mikä heikentää tietoturvaa ja yhteensopivuutta. Lisäksi varaosien saatavuus alkaa vähentyä, huoltopalvelut voivat päättyä ja korvaavien komponenttien hankinta vaikeutuu. Tämä vaihe merkitsee käytännössä sitä, että järjestelmä ei enää ole valmistajan tuen piirissä, mikä lisää riskejä ja kustannuksia.
- Laiteohjelmistojen ja käyttöohjelmistojen päivitykset
  - Päivitysten saatavuus ja yhteensopivuus uusien ohjelmistoversioiden kanssa vaikuttavat käyttöikään ja tietoturvaan.
- Huoltopalveluiden saatavuus
  - Toimittajan kyky tarjota huoltoa ja varaosia koko elinkaaren ajan on kriittinen järjestelmän toimivuudelle.
- Yhtenäinen laitekanta
  - Standardoidut komponentit helpottavat hallintaa ja huoltoa, vähentävät kustannuksia ja nopeuttavat korjaustoimia.
- Dokumentaation ajantasaisuus
  - Tarkat asennus-, huolto- ja konfiguraatiodokumentit varmistavat hallitun ylläpidon ja nopean reagoinnin häiriötilanteissa.
- Integraatiot ja rajapinnat

  - Järjestelmien yhteensopivuus muiden turva- ja kiinteistöjärjestelmien kanssa vaikuttaa elinkaareen ja päivitystarpeisiin.
- Tietoturva ja kyberturvallisuus
  - Kyberturvallisuusvaatimukset ja haavoittuvuuksien hallinta voivat lyhentää käyttöikää, jos järjestelmä ei täytä uusia vaatimuksia.
- Käyttöympäristön muutokset
  - Rakenteelliset muutokset, laajennukset tai riskiprofiilin muutos voivat edellyttää järjestelmän uudistamista. Lisäksi käyttöympäristön fyysiset olosuhteet, kuten muuttuvat sääolosuhteet, kosteus, lämpötilavaihtelut ja vuodenajat, voivat vaikuttaa komponenttien kulumiseen, korroosioon ja järjestelmän toimintavarmuuteen.
- Lainsäädäntö ja standardit
  - Lakisääteiset tarkastusvelvoitteet ja standardien päivitykset voivat pakottaa järjestelmän modernisointiin.
- Käyttäjäkoulutus ja osaaminen
  - Riittävä koulutus ja käyttöohjeet varmistavat järjestelmän oikean käytön ja vähentävät virheistä johtuvia vikaantumisia.
- Budjetointi ja PTS-suunnitelmat
  - Järjestelmien sisällyttäminen pitkäjänteiseen investointisuunnitteluun varmistaa resurssien saatavuuden ajoissa.

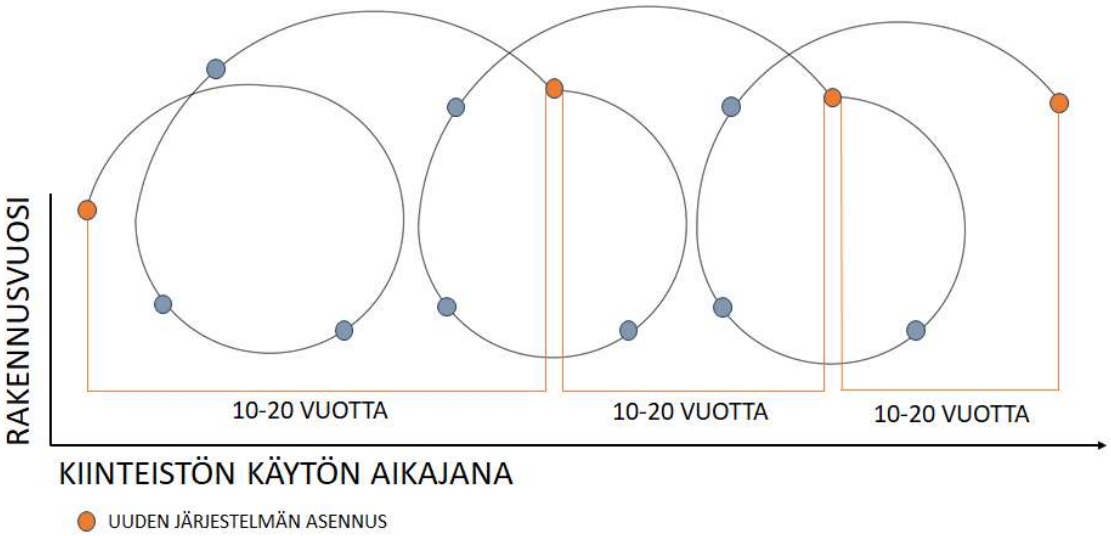
Kuvassa 20 on esitetty teknisen järjestelmän elinkaari asennuksesta uusintaan. Järjestelmän asennuksen ja käyttöönottoon (1) sekä käyttäjäkoulutuksen jälkeen alkaa käyttövaihe (2), jonka aikana järjestelmää tyypillisesti päivitetään ja laajennetaan. Järjestelmän elinkaaren loppupuolella tulee ryhtyä hyvissä ajoin valmistelemaan vanhan järjestelmän korvaamista modernimmalla (3). Hankintavaiheen päätteeksi uusi järjestelmä on hankittu (4) ja alkaa uuden järjestelmän asennus- ja käyttöönottovaihe (5).



Kuva 20 Teknisen järjestelmän elinkaari

Ajantasaisen dokumentaation merkitys korostuu järjestelmää uusittaessa (esitetty alla olevassa kuvassa 21 oranssilla ympyrällä). Uuden järjestelmän asennuksen jälkeen sen dokumentaatio on kattavaa ja ajan tasalla (järjestelmän laajuus, kaapeloinnit, laitteet,

integraatiot ym). Mikäli dokumentaatiota pidetään yllä ja siihen lisätään toteutetut päivitykset ja laajennukset, on uuden järjestelmän hankintaa varten käytettävissä kattava dokumentaatio nykytilasta.



Kuva 21 Teknisten järjestelmien elinkaari suhteessa kiinteistön käyttöikään

5.6.2 Esimerkki fyysisen turvallisuuden vuosikellosta

Kuukausi	Johtaminen ja seuranta	Riskien arviointi	Tekninen ylläpito	Henkilöstö ja osaaminen	Auditointi ja kehittäminen
Tammi	Turvallisuuden vuosisuunnittelu	Riskikartan päivitys	Turvajärjestelmien kuntotarkastus	Turvallisuusperehdytys (vuoden aloitus)	Kehitystoimenpiteiden suunnittelu
Helmi	Raportointi johdolle	Riskien tunnistamisen tarkennus	Hälytysjärjestelmien testaus	Turvallisuusteemat / viestintä	Auditointisuunnitelma
Maali	Q1-tilannekatsaus	Riskien arvioinnin tarkastus	Kamera- ja kulunvalvontajärjestelmien tarkastus	Turvavartit / osaamisen ylläpito	Sisäinen auditointi
Huhti	Johdon katselmus	Kriittisten kohteiden arviointi	Lukitus- ja avainhallinnan tarkastus	Koulutukset	Poikkeamien analyysi
Touko	Seuranta	Riskien käsittelytoimenpiteiden päivitys	Huollot ja korjaavat toimenpiteet	Turvallisuusviestintä	Kehitystoimien seuranta
Kesä	Kevyt seuranta	Riskien seuranta (kesäajan erityisriskit)	Kenttäkohteiden tarkastukset	Kesäajan ohjeistus	-
Heinä	Kevyt seuranta	Riskien seuranta	Kriittisten kohteiden tarkastus	-	-
Elo	Q2–Q3 katsaus	Riskien päivitys	Järjestelmien testaus	Käynnistyskoulutukset	Sisäinen arviointi
Syys	Johdon raportointi	Riskien arviointi (vuosipäivitys)	Turvatekniikan huolto	Turvallisuusteemat	Auditointi
Loka	Q3-katsaus	Riskien priorisointi	Hälytysjärjestelmien testaus	Turvallisuusviikko	Auditointitulosten käsittely
Marras	Seuraavan vuoden suunnittelu	Riskikartan päivitys	Investointitarpeiden arviointi	Koulutukset	Kehitystoimet
Joulu	Vuosiyhteenveto	Riskienhallinnan arviointi	Järjestelmien tarkistus	Henkilöstöviestintä	Vuosiarviointi

Kuva 22: Esimerkki fyysisen turvallisuuden vuosikellosta

6 POIKKEUSOLOIHIN VARAUTUMINEN

Luvussa 4.9 on käsitelty organisaation varautumista normaalioloissa. Erotuksena häiriö- ja kriisitilanteiden määritelmiin, ovat poikkeusolot yhteiskunnallinen, valtion ylimmän johdon julistama tila. Valmiuslaissa todetaan, että yhteiskunta siirtyy poikkeusoloihin, kun valtioneuvosto ja tasavallan presidentti toteavat yhteiskunnan tilanteen sellaiseksi, että siihen kohdistuvia häiriöitä ei pystytä saamaan hallintaan viranomaisten normaalein toimivaltuuksin ja valtioneuvosto antaa käyttöönottoasetuksen, jonka eduskunta hyväksyy. Poikkeusoloissa otetaan käyttöön tavanomaisesta poikkeava lainsäädäntö, joka antaa lisää toimivaltuuksia viranomaisille.

Suomessa on käytössä kokonaisturvallisuuden malli, joka kuvataan kokonaisuudessaan Valtioneuvoston julkaisemassa Yhteiskunnan turvallisuusstrategiassa. Kokonaisturvallisuuden toimintamallissa yhteiskunnan elintärkeistä toiminnoista huolehditaan yhteistoimintana viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten kesken. Vastuu yhteiskunnan turvallisuuden ylläpidosta ja varmistamisesta on siis jaettu koko yhteiskunnan eri toimijoille ja tämä luo perustan suomalaisen yhteiskunnan kriisinkestävyydelle eli resilienssille.

Elinkeinoelämän osalta tämä tarkoittaa sitä, että yksittäiset, huoltovarmuuskriittiset yritykset vastaavat osaltaan siitä, että yhteiskunnan toiminnat pysyvät käynnissä kaikissa tilanteissa. Keskeinen tekijä tässä on kansallinen kriittinen infrastruktuuri, joka on suunniteltu toimimaan erilaisissa häiriötilanteissa.

Valmiuslain (1552/2011) mukaan poikkeusoloja ovat:

1) Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila,
2) Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii valmiuslain mukaisten toimivaltuuksien välitöntä käyttöön ottamista,
3) väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat,
4) erityisen vakava suuronnettomuus ja sen välitön jälkitila, sekä
5) vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti.

Valmiuslain kokonaisuudistus on ollut vireillä tätä oppaan julkaisun aikana ja oppaan tiedot perustuvat oppaan julkaisuajankohtana voimassa olleeseen valmiuslakiin.

6.1 MITEN VARAUDUTAAN?

Fyysisen suojauksen kannalta keskeiset asiat ovat käsitelty normaaliolojen varautumisessa. Luvussa 4.9 käsitellään normaalitilanteen varautumisen perusasiat. Mikäli näistä on huolehdittu ennakkoon, jää jäljelle kysymys siitä, mihin varautua, kun tilanne on käynnissä. Keskeinen kysymys on, miten vedenjakelu koko matkalta turvataan raakavesilähteeltä loppukäyttäjille. Miten varmistetaan, että poikkeusoloissa kaikilla alueen vesilaitoksilla on riittävä kapasiteetti? Miten hoidetaan varavedenjakelu? Varautumisen kannalta oleellista on, että normaaliolojen varautuminen luo pohjan poikkeusoloihin varautumiselle.

Poikkeusoloihin varautumisen tavoitteena on turvata kriittisen infrastruktuurin, vesihuollon toimitusvarmuuden sekä henkilöstön ja asiakkaiden turvallisuus myös olosuhteissa, joissa uhkamallit ja ympäristö poikkeavat merkittävästi normaalioloista.

Kohteiden lisäsuojaus

Poikkeusoloissa kohteisiin voi kohdistua sekä suoria että epäsuoria vaikutuksia, kuten räjähdysvaikutuksia, sirpaleita, iskuaaltoja, fyysisiä hyökkäyksiä tai häiriöitä teknisiin järjestelmiin. Varautumisen tulisi sisältää:

- Tilapäiset rakenteelliset lisäsuojaukset, joilla voidaan pienentää pommitusten, drone-iskujen tai sabotaasin vaikutuksia (esim. suojaseinämät, betonisuojaelementit, maa-ainesvallien hyödyntäminen, ajoneuvohidasteet).
    - Huomioitava valmius siirtää tilapäisiä rakenteellisia lisäsuojauksia alueella tarvittavan kaluston avulla.
- Tärkeimpien sisäänkäyntien, teknisten tilojen, varavoimageneraattoreiden ja valvomon vahventaminen tai suojaaminen (luodinkestävyys, sirpalesuojaus, painevaikutukselta suojaaminen).
- Kriittisten prosessien ja laitteiden hajauttaminen mahdollisuuksien mukaan, jotta yksittäisen iskun vaikutukset pysyvät rajattuina.
- Kulkuväylien järjestelyt siten, että ne eivät mahdollista suoraa ajolinjaa kriittisiin rakennuksiin (raskaat ajoesteet, betoniporsaat tai maavallit)
- Fyysiset drone-esteet kuten verkot, suojarakenteet ja katosratkaisut kriittisten laitteiden ja kattoelementtien ylle.

Sähköä ja tiedonsiirtoa vaativien järjestelmien toimintavarmuus

Fyysiset suojaus- ja valvontajärjestelmät ovat usein riippuvaisia sähkönsyötöstä ja tietoliikenneyhteyksistä. Poikkeusoloihin varautumisen tulee sisältää:

- Varavoiman riittävä mitoitus ja polttoainehuollon varmistaminen pidempikestoisiin häiriöihin.
- Tietoliikenneyhteyksien varmentaminen, kuten rinnakkaiset yhteystavat (kiinteä, 4G/5G, satelliitti).
- Mahdollisuus siirtyä manuaalisiin toimintamalleihin, jos automaatiojärjestelmät häiriintyvät.

Henkilöstön toimintavalmius poikkeusoloissa

Rakenteellisten ja teknisten toimenpiteiden lisäksi keskeistä on henkilöstön osaaminen ja toimintakyky:

- Koulutus poikkeusolojen toimintamalleihin.
- Selkeät roolit ja vastuut kriisitilanteessa.
- Harjoitukset ja valmiuden testaus.
- Uhkatilanteiden kiristyessä kohteiden suojaaminen edellyttää normaalia korkeampaa valvontatasoa, jota voidaan toteuttaa esimerkiksi tehostetulla vartioinnilla

Huomiona, että poikkeusoloissa henkilöstöresurssit, kuten ulkoistetut vartioimispalvelut, voivat muodostua nopeasti niukoiksi. Ulkoisilta toimijoilta ei välttämättä ole mahdollista saada lisäresurssia, jolloin organisaation on varauduttava hoitamaan keskeiset tehtävät omalla henkilöstöllään.

6.2 VALMIUS KORJATA MATERIAALISIA TUHOJA

Ukrainassa on panostettu valmiuteen korjata nopeasti iskujen aiheuttamia tuhoja. Rasmussenin raportissa mainitaan, että keskeisiä asioita erityisesti pienempien vesivoimaloiden osalta on sen pohtiminen, miten henkilöstön suojaaminen järjestetään sekä mahdollisuus ohjata laitosta etäkäytön avulla.

Logistiikkareittien katkeaminen voi tilanteesta riippuen vaikuttaa varaosien ja laitteiden saatavuuteen. Siksi kriittisten osien varmuusvarastointi ja vanhojen, käytöstä poistettujen mutta toimivien laitteiden säästäminen varaosiksi, korvaavien ratkaisujen pohtiminen ja ostojen hajauttaminen eri laitetoimittajille ovat keinoja vähentää riippuvuutta laitetoimittajiin. Laitetoimittajaan liittyvä riski voi realisoitu myös Suomen ulkopuolella tapahtuvista syistä, kuten logistiikkaketjuihin vaikuttavista geopoliittisista muutoksista tai laitetoimittajan konkurssista.

6.3 RESURSSIT POIKKEUSOLOISSA

Laaja ja vakava yhteiskunnallinen tilanne voi vaikuttaa työntekijöiden saatavuuteen eri tavoin ja eri syistä. Esimerkiksi Rasmussen Globalin raportissa todetaan, hyökkäyssodan käynnistyttyä osa ukrainalaisista lähti rintamalle ja osa pakeni ulkomaille. COVID-19-pandemian aikana sairastumiset ja liikkumisrajoitukset vaikuttivat työntekijöihin. Työntekijän lähipiirissä voi olla henkilö, joka tarvitsee erityisen paljon tukea häiriötilanteessa niin, että työntekijä jää pois töistä. Lisäksi häiriötilanteet ovat yksilöille henkisesti kuormittavia varsinkin pitkään jatkuessaan.

Häiriötilanteen vaikutuksia oman organisaation henkilöresursseihin on hyvä pohtia. Henkilövarausten tekeminen on keino estää organisaation toiminnan kannalta kriittisen henkilöstön otto puolustusvoimien käyttöön.

- Miten toimitaan häiriötilanteessa, jossa henkilövarattu työntekijä - tai ylipäänsä henkilöstö - ei saavukaan töihin?
- Miten toiminta järjestetään, jos oman organisaation ja sidosryhmien työntekijöiden määrä vähenee äkillisesti?
- Onko omassa organisaatiossa riittävää osaamista kriittisimpien tehtävien suhteen?
- Miten kohteen vartiointi järjestetään, jos vartioimisliikkeellä ei ole tarjota työntekijöitä?

Poikkeustilanteen ollessa käynnissä on mahdollista, että viranomainen joutuu priorisoimaan resurssiensa käyttöä tiettyihin kohteisiin, jolloin muut kohteet joutuvat pärjäämään itsenäisesti.

6.3.1 Henkilövaraukset

Kun puhutaan VAP-varauksista, tarkoitetaan henkilövarauksia. Henkilövaraus perustuu asevelvollisuuslain 89 §:ään ja sen avulla yhteiskunnan toiminnan kannalta kriittiset organisaatiot voivat varata kriittistä henkilöstöä käyttöönsä poikkeusolojen kaltaisissa kriisitilanteissa. Jos työntekijästä on tehty henkilövaraus, hänen sodan ajan tehtävänsä on toimia työnantajansa palveluksessa yhteiskunnan elintärkeiden toimintojen turvaamiseksi.

Asevelvollisuuslain 89 §:ssä todetaan:

”Asianomaisen viraston, laitoksen, yhteisön tai muun työnantajan hakemuksesta liikekannallepanon varalta palvelukseen voidaan jättää määräajaksi tai toistaiseksi kutsumatta julkisoikeudellisessa palvelussuhteessa tai siihen rinnastettavassa tehtävässä olevia, erityisen ammatin harjoittajia sekä muita, joiden palvelukseen kutsuminen saattaisi vaarantaa puolustusvoimien varustamista tai ylläpitoa, yleistä taloutta tai muita yleisiä etuja.”

Henkilövarausta haetaan siten, että varattavan henkilön työnantaja täyttää varaushakemuksen ja toimittaa sen puolustusvoimien aluetoimistolle, joka on vastuussa varaavan organisaation kotipaikkakunnasta. Aluetoimisto tekee päätöksen asevelvollisten suhteen, siviilipalveluskeskus vastaa siviilipalvelusvelvollisia koskevista varaushakemuksista.

On tärkeää huomioida, että huoltovarmuuskriittiset yritykset voivat itse esittää omaa henkilöstöään varattavaksi, mutta vesilaitoksen tulee tehdä esitykset niiden palveluntuottajien henkilöiden osalta, joiden yritykset eivät voi itse tehdä varausesityksiä.

Maanpuolustuskoulutus MPK tarjoaa verkkokurssia *”Henkilövaraaminen poikkeusolojen tehtäviin (VAP)”*. Koulutus antaa perustiedot siitä, mitä henkilövaraaminen poikkeusolojen tehtävään tarkoittaa. (Puolustusvoimat 2025)

6.3.2 Autojen ja työkoneiden varaaminen

Autoja ja työkoneita on mahdollista varata organisaation omaan käyttöön ATV-toimintamallia hyödyntäen. Poikkeusoloissa armeija tarvitsee siviilipuolelta käyttöönsä kuljetuskalustoa. Yhteiskunnan kriittisten logististen ketjujen ja toimintojen turvaamiseksi organisaatioiden on mahdollista tehdä ATV-varauksia ajoneuvoistaan ja laitteistaan.

Kuten yllä, myös tässä asiassa huoltovarmuuskriittiset yritykset voivat itse esittää omaa kalustoaan varattavaksi, mutta vesilaitoksen tulee tehdä esitykset niiden palveluntuottajien kaluston osalta, joiden yritykset eivät voi itse tehdä varausesityksiä.

7 LÄHTEET

Liite 1 sisältää listauksen oppaan työstössä hyödynnetyistä laista ja asetuksista, standardeista, eri tahojen julkaisemista ohjeista sekä vesihuoltoalan omista ohjeistusta.

Design for Security. 2026. What is 'Crime Prevention Through Environmental Design'? Verkkojulkaisu.
https://designforsecurity.org/crime-prevention-through-environmental-design/

Liikenne- ja viestintävirasto Traficom. Määräys 65 kiinteistön sisäverkoista ja teleurakoinnista.
https://www.traficom.fi/fi/saadokset/maarays-65-kiinteiston-sisaverkoista-ja-teleurakoinnista

Liikenne- ja viestintävirasto Traficom. Kiinteistöjen laitetilojen lukitus. Liikenne- ja viestintäviraston suosituksia. 306/2019 S. Voimaantulopäivä: 12.11.2019.
https://www.traficom.fi/sites/default/files/media/regulation/FI_Suositus_306_2019_S.pdf

Puolustusvoimat. 2025. Henkilövaraaminen poikkeusolojen tehtäviin -verkkokurssi on julkaistu. Tiedote. Julkaisuajankohta: 8.10.2025 13.44
https://puolustusvoimat.fi/-/henkilovaraaminen-poikkeusolojen-tehtaviin-verkkokurssi-on-julkaistu

Rikoksentorjuntaneuvosto. 2025 A. Rikoksentorjunta kaupunkisuunnittelun keinoin (CPTED). Verkkojulkaisu.
https://rikoksentorjunta.fi/rikoksentorjunta-kaupunkisuunnittelun-keinoin

Rikoksentorjuntaneuvosto. 2025 B. Turvallisuuslähtöinen suunnittelu – Tampereen Muotialan asuinalue. Verkkojulkaisu.
https://rikoksentorjunta.fi/turvallisuuslahtoinen-suunnittelu

Sanastokeskus TSK. 2017.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Vesilaitosyhdistys. 2021. Turvallisuusjohtaminen vesihuoltolaitoksilla.
https://www.vesilaitosyhdistys.fi/verkkokauppa/tuotteet/turvallisuusjohtaminen-vesihuoltolaitoksilla/

Yrityssuojeluyhdistys. KTL1E-lukitusjärjestelmä.
https://www.yrityssuojelu.fi/ktl1e-lukitusjarjestelma

https://rikoksentorjunta.fi/turvallisuuslahtoinen-suunnittelu
https://www.cpted.net/Primer-in-CPTED

Design for Security. 2026. What is 'Crime Prevention Through Environmental Design'? Verkkojulkaisu.
https://designforsecurity.org/crime-prevention-through-environmental-design/

8 KUVA- JA TAULUKKOLUETTELO

Kuva 1: Elinkeinoelämän keskusliiton kehittämä yritysturvallisuusmalli 11
Kuva 2: Elinkeinoelämän keskusliiton kehittämä yritysturvallisuusmatriisi 11
Kuva 3: Oppaan käyttö nykytilan tunnistamisen jälkeen 12
Kuva 4: Turvallisuuden peruselementit 12
Kuva 5 Organisaation suojattavat arvot 13
Kuva 6 Turvallisuuspolitiikka ja turvallisuuden osa-alueet 16
Kuva 7: Tilaluokkien yhteydet erilaisiin kulkuoikeuksiin 18
Kuva 8 Riskienhallinta ja riskien arviointiprosessi 30
Kuva 9: PDCA-malli (Plan-Do-Check-Act) 31
Kuva 10 Toimintaympäristön määrittäminen 31
Kuva 11 Riskien arviointiprosessi 32
Kuva 12 Riskien käsittely 33
Kuva 13: Fyysisen turvallisuuden keinovalikoima ja niiden ominaisuudet 36
Kuva 14: Tyypilliset suojattavat arvot ja niihin kohdistuvat uhkat 36
Kuva 15: Teknisten ja rakenteellisten ratkaisujen sekä vartioinnin käyttötarkoitukset fyysisessä suojautumisessa 37
Kuva 16: Esimerkkikuvaus eri toimintojen riippuvuussuhteista ja vaikutuksesta fyysisen turvallisuuden toteutumiseen 38
Kuva 17: Kolmiportainen luokittelu kohteen kriittisyyden arviointia varten 40
Kuva 18 Kehäsuojausmallin vyöhykkeet 42
Kuva 19 Normaaliolojen ja poikkeusolojen ero. 60
Kuva 20 Teknisen järjestelmän elinkaari 74
Kuva 21 Teknisten järjestelmien elinkaari suhteessa kiinteistön käyttöikään 75
Kuva 22: Esimerkki fyysisen turvallisuuden vuosikellosta 75

Taulukko 1: Turvallisuuden parantamisen kustannustehokkaat vaihtoehdot 37

LIITTEET

LIITE 1 OHJAAVAT MUUT ASIAKIRJAT
LIITE 2 FYYSISEN TURVALLISUUDEN HINTA-ARVIOT
LIITE 3 KEHÄSUOJAUSMALLIN ESIMERKKIRATKAISUT
LIITE 4 KULUNHALLINNAN JA PÄÄSYNHALLINNAN PERIAATTEET
LIITE 5 VESIHUOLTOLAITOKSEN NYKYTILAN ESIARVIOINTI
LIITE 6 TYÖKALU FYYSISEN TURVALLISUUDEN ARVIOINTIIN

Liitteiden tietoluokka:
TLP Amber - Rajattu organisaatioiden sisäinen käsittely

Liitteet ovat Vesilaitosyhdistyksestä vesihuoltolaitosten saatavilla.