OHJE YVL A.12

YDINLAITOKSEN TIETOTURVALLISUUDEN HALLINTA

Määritelmät

Valtuutusperusteet

Ydinenergialain (990/1987) 7 r §:n mukaan Säteilyturvakeskuksen tehtävänä on asettaa ydinenergialain mukaisen turvallisuustason toteuttamista koskevat yksityiskohtaiset turvallisuusvaatimukset.

Soveltamissäännöt

YVL-ohjeen julkaiseminen ei sinänsä muuta Säteilyturvakeskuksen ennen ohjeen julkaisemista tekemiä päätöksiä. Vasta kuultuaan asianosaisia Säteilyturvakeskus antaa erillisen päätöksen siitä, miten uutta tai uusittua YVL-ohjetta sovelletaan käytössä tai rakenteilla oleviin ydinlaitoksiin ja luvanhaltijoiden toimintoihin. Uusiin ydinlaitoksiin ohjeita sovelletaan sellaisenaan.

Kun Säteilyturvakeskus harkitsee YVL-ohjeissa esitettyjen, uusien turvallisuusvaatimuksien soveltamista käytössä tai rakenteilla oleviin ydinlaitoksiin, se ottaa huomioon ydinenergialain (990/1987) 7 a §:ssä säädetyt periaatteet: *Ydinenergian käytön turvallisuus on pidettävä niin korkealla tasolla kuin käytännöllisin toimenpitein on mahdollista. Turvallisuuden edelleen kehittämiseksi on toteutettava toimenpiteet, joita käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehittyminen huomioon ottaen voidaan pitää perusteltuina.*

Ydinenergialain 7 r §:n kolmannen momentin mukaan *Säteilyturvakeskuksen turvallisuusvaatimukset velvoittavat luvanhaltijaa, kuitenkin niin, että luvanhaltijalla on oikeus esittää muunkinlainen kuin vaatimuksissa edellytetty menettelytapa tai ratkaisu. Jos luvanhaltija vakuuttavasti osoittaa, että esitetty menettelytapa tai ratkaisu toteuttaa tämän lain mukaisen turvallisuustason, Säteilyturvakeskus voi sen hyväksyä.*

Uusien ydinlaitosten osalta tämä ohje on voimassa 1.3.2021 alkaen toistaiseksi. Rakenteilla olevilla ja käyvillä ydinlaitoksilla tämä ohje saatetaan voimaan erillisellä STUKin päätöksellä. Ohje kumoaa ohjeen YVL A.12 (22.11.2013).

STUK • SÄTEILYTURVAKESKUS
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY
Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FI-00811 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

1 Johdanto

101. Tässä ohjeessa annetaan vaatimuksia ydinlaitoksen tietoturvallisuuden hallinnalle ja täsmennetään STUKin määräyksessä ydinenergian käytön turvajärjestelyistä (STUK Y/3/2020) säädettyjä suunnitteluvaatimuksia. Määräyksen STUK Y/3/2020 4 §:n 5 kohdan mukaan *järjestelmien ja laitteiden suunnittelussa ja ylläpidossa on käytettävä tarkoituksenmukaisia tietoturvallisuusperiaatteita. Turvallisuuden kannalta tärkeitä järjestelmiä ja laitteita koskevan luvattoman toiminnan ja tietoturvallisuuspoikkeamien havaitsemiseksi ja estämiseksi sekä vahingollisten seurausten rajoittamiseksi on oltava tarkoituksenmukaiset menetelmät ja niitä koskevat suunnitelmat.* Määräyksen STUK Y/3/2020 4 §:n 6 kohdan mukaan *ydinenergian käytössä on varauduttava tietoturvallisuusuhkista johtuvien poikkeavien tilanteiden hallintaan.* **[**2021-02-12 **]**

102. Turvajärjestelyjä, mukaan lukien tietoturvallisuus, koskevien asiakirjojen julkisuudesta on voimassa se, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) [4] säädetään. Vaitiolovelvollisuudesta ja velvollisuudesta suojata tietoa säädetään ydinenergialain (990/1987) [1] 78 §:ssä. **[**2021-02-12 **]**

103. Turvajärjestelyjä koskevat yleiset velvoitteet esitetään ydinenergialaissa (990/1987) ja sen nojalla annetuissa Säteilyturvakeskuksen määräyksissä ydinenergian käytön turvajärjestelyistä (STUK Y/3/2020) [2] ja ydinvoimalaitoksen turvallisuudesta (STUK Y/1/2018) [3]. Velvoitteita sisältyy myös Suomen tekemiin kansainvälisiin ydinenergia-alan sopimuksiin, hallitusten välisiin muihin sopimusjärjestelyihin sekä Suomen antamiin sitoumuksiin. Suunnitteluperusteuhka (DBT) on esitetty erillisessä asiakirjassa ”Ydinenergian ja säteilyn käytön suunnitteluperusteuhka”, joka toimitetaan ohjeessa YVL A.11 ”Ydinlaitoksen turvajärjestelyt” määriteltyjen laitosluokkien luvanhaltijoille käytettäväksi turvajärjestelyjen ja tietoturvallisuuden hallinnan suunnittelun perusteena. STUKin ohjeet YVL A.11 ja YVL A.12 yhdessä edellä mainittujen asiakirjojen kanssa muodostavat perustan ydinlaitosten turvajärjestelyille. Ydinlaitosten turvajärjestelyjä valvovana viranomaisena toimii ydinenergialain 55 §:n mukaisesti Säteilyturvakeskus (STUK). Turvajärjestelyistä vastaa ydinenergialain 9 §:n mukaisesti luvanhaltija siltä osin, kuin nämä tehtävät eivät kuulu viranomaisille. **[**2021-02-12 **]**

104. Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, laitteiden, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa. Tietojen eheyttä, saatavuutta ja luottamuksellisuutta suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. Tietoturvallisuus on osa luvanhaltijan johtamisjärjestelmää ja turvajärjestelyjä. **[**2021-02-12 **]**

105. Tietoturvallisuus kattaa tiedon eheyden, saatavuuden ja luottamuksellisuuden turvaamisen sen kaikissa olomuodoissaan aina tiedon luomisesta sen tuhoamiseen asti. **[**2021-02-12 **]**

2 Soveltamisala

201. Tässä ohjeessa esitetään ydinlaitoksen rakentamis- tai käyttölupaa hakevan sekä ydinlaitosta rakentavan tai käyttävän organisaation tietoturvallisuutta koskevat määräykset ja niiden soveltamista koskevat vaatimukset. Ohjetta sovelletaan ydinlaitoksiin niiden elinkaaren kaikissa vaiheissa. Ohje on tarkoitettu ydinlaitosten luvanhakijoille ja luvanhaltijoille, ja sitä sovelletaan organisaatioihin, joilla on vaikutusta ydinlaitosten tietoturvallisuuteen. Muuhun ydinenergian käyttöön ohjeesta sovelletaan lukuja 1, 2 ja 3, pois lukien vaatimukset 324, 325 ja 326. Tietoturvallisuuden kannalta tärkeitä vaatimuksia ja STUKin suorittamaa valvontaa kuvataan myös A-sarjan YVL-ohjeissa sekä ohjeissa

- B.1 Ydinvoimalaitoksen turvallisuussuunnittelu
- B.2 Ydinvoimalaitoksen järjestelmien, rakenteiden ja laitteiden luokittelu
- B.7 Varautuminen sisäisiin ja ulkoisiin uhkiin ydinlaitoksessa
- C.5 Ydinvoimalaitoksen valmiusjärjestelyt
- E.7 Ydinlaitoksen sähkö- ja automaatiolaitteet.

[2021-02-12 **]**

3 Tietoturvallisuuden hallinta

3.1 Tietoturvallisuuden hallintajärjestelmä

301. Luvanhaltijan johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintaan. **[**2021-02-12 **]**

302. Luvanhaltijalla on oltava tietoturvallisuuden hallintajärjestelmä, joka on osa johtamisjärjestelmää. **[**2021-02-12 **]**

303. Standardin SFS:EN ISO/IEC 27000 [19] mukaan *tietoturvallisuuden hallintajärjestelmä koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista tai toiminnoista joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan*. **[**2021-02-12 **]**

303a. Tietoturvallisuuden hallintajärjestelmän on katettava toimenpiteet ja menettelyt valita, toteuttaa ja parantaa asianmukaisia hallintakeinoja. **[**2021-02-12 **]**

303b. Tietoturvallisuuden hallintajärjestelmän on katettava ulkoisten resurssien ohjaaminen ja valvonta tietoturvallisuuden osalta. **[**2021-02-12 **]**

304. Kansainväliset tietoturvallisuuden standardit ja ohjeistukset [19] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin. **[**2021-02-12 **]**

304a. Kansalliset ohjeistukset [9, 10, 13] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin. **[**2021-02-12 **]**

305. Ohje YVL A.11 esittää vaatimuksen tilannekuvan välittämisestä. Tilannekuvan välittämisessä on huomioitava tietoturvallisuus, siten ettei tietoturvallisuudesta huolehtiminen saa vaarantaa ajantasaisen tilannekuvan välittämistä. **[**2021-02-12 **]**

306. Säteilyturvakeskuksen määräysten STUK Y/1/2018 25 §:n ja STUK Y/4/2018 38 §:n mukaisesti *ydinlaitosta suunniteltaessa, rakennettaessa, käytettäessä ja käytöstä poistettaessa on ylläpidettävä hyvää turvallisuuskulttuuria*. Tietoturvallisuudesta huolehtiminen on osa hyvää turvallisuuskulttuuria. **[**2021-02-12 **]**

307. Suunnitteluperusteuhka (DBT) määrittelee uhkan, jota käytetään turvajärjestelyjen vaatimusten, suunnittelun ja arvioinnin perusteena. Luvanhaltijan on suunniteltava tietoturvallisuuden hallintajärjestelmänsä siten, että tietoturvallisuuteen liittyvä suunnitteluperusteuhka voidaan torjua suunnitteluperusteuhka-asiakirjassa asetettujen suojaustavoitteiden mukaisesti niin hyvin kuin käytännöllisin toimenpitein on mahdollista. **[**2013-11-22 **]**

308. Luvanhaltijan on määriteltävä tietoturvallisuuden hallintapolitiikka, joka voi olla itsenäinen asiakirja tai osa laajempaa kokonaisuutta. **[**2021-02-12 **]**

309. Tietoturvallisuuden tavoitteet on esitettävä osana tietoturvallisuuden hallintajärjestelmää. **[**2021-02-12 **]**

309a. Tietoturvallisuustavoitteiden saavuttamista on seurattava ja tavoitteita on arvioitava jatkuvan parantamisen periaatetta noudattaen. **[**2021-02-12 **]**

310. Tietoturvaorganisaatio on kuvattava tietoturvallisuuden hallintajärjestelmässä. Kuvauksessa on otettava huomioon myös ulkoiset toimijat ja näiden vastuut. **[**2021-02-12 **]**

310a. Tehtävät ja vastuualueet on tarpeen mukaan eriytettävä, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. **[**2021-02-12 **]**

311. Viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen on käytettävä valtioneuvoston asetuksen (1101/2019) [20] ja neuvoston päätöksen (2013/488/EU) [21] mukaisia menettelyjä. Ohjeistusta saa esimerkiksi VAHTI-ohjeista [9]. Suojauksen tietoturvallisuuden arviointiin voidaan käyttää esimerkiksi KATAKRI-kriteeristöä [13]. **[**2021-02-12 **]**

311a. Valtioneuvoston asetuksen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) 6 §:n mukaisesti *valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle.* Ennen viranomaisen turvallisuusluokittelemaa, salassa pidettävää tai näistä johdettua tietoa sisältävän aineiston luovuttamista kolmannelle osapuolelle luvanhaltijalla tulee olla Säteilyturvakeskuksen hyväksyntä tiedon luovuttamiselle. **[**2021-02-12 **]**

312. Luvanhaltijalla on oltava menettelyt tietoturvallisuuden riskien arviointiin ja hallintaan. **[**2021-02-12 **]**

312a. Luvanhaltijan on varmistettava, että tietoturvallisuuden riskien arviointiin käytetyt menettelyt ovat riittävät ja merkittävät riskit on tunnistettu. **[**2021-02-12 **]**

313. Poistettu. **[**2021-02-12 **]**

314. Luvanhaltijan on tehtävä tietoturvallisuuden uhka- ja riskienarviointi, ja se on päivitettävä säännöllisesti ja merkittävien tietoturvallisuutta koskevien tapahtumien, muutosten tai uusien uhkien ilmentyessä. **[**2021-02-12 **]**

315. Tietoturvallisuuden uhkat ja riskit on systemaattisesti analysoitava, ja suojaavat toimenpiteet ja menetelmät on valittava analyysin perusteella. **[**2021-02-12 **]**

316. Suojattavat kohteet on tunnistettava ja määriteltävä riittävän yksityiskohtaisesti. **[**2021-02-12 **]**

316a. Suojattaviin kohteisiin liittyvät uhkat ja haavoittuvuudet sekä tietoturvallisuustapahtumien aiheuttamat vaikutukset on arvioitava ja niiden perusteella on määriteltävä tarpeelliset suojaustoimenpiteet. **[**2021-02-12 **]**

316b. Suojaustoimenpiteet on dokumentoitava. **[**2021-02-12 **]**

317. Siirretty numeroille 419a ja 419b. **[**2021-02-12 **]**

3.2 Tiedon suojaamista koskevat vaatimukset

318. Asiakirjoja koskevat yleiset vaatimukset on esitetty ohjeissa YVL A.1 ”Ydinenergiankäytön turvallisuusvalvonta”, YVL A.3 ”Turvallisuuden johtaminen ydinalalla” ja YVL A.11 ”Ydinlaitoksen turvajärjestelyt”. **[**2021-02-12 **]**

319. Tieto on luokiteltava sen tietoturvallisuus- ja turvallisuusmerkityksen mukaan. **[**2021-02-12 **]**

319a. Tietoa on suojattava luokituksen mukaisesti luvattomalta käytöltä, muuttamiselta ja tuhoamiselta. Tiedon saatavuus luvalliselle käyttäjälle on turvattava. **[**2021-02-12 **]**

3.3 Resurssien hallinta

320. Ohjeet YVL A.4 ”Ydinlaitoksen organisaatio ja henkilöstö” ja YVL A.11 ”Ydinlaitoksen turvajärjestelyt” osoittavat yleiset vaatimukset resurssien hallinnan osalta. Resurssien on katettava henkilöstöresurssit, tarvittava osaaminen sekä työkalut. **[**2021-02-12 **]**

320a. Luvanhaltijan on huolehdittava siitä, että sillä on käytettävissään riittävät resurssit ja osaaminen tietoturvallisuuden hallinnan suunnitteluun, toteuttamiseen, arviointiin ja jatkuvaan parantamiseen. **[**2021-02-12 **]**

321. Keskeisten tietoturvallisuuden hallintaan liittyvien henkilöiden ja muiden resurssien on oltava luvanhaltijan palveluksessa tai omistuksessa. **[**2021-02-12 **]**

321a. Ennen kuin tietojärjestelmien ylläpito-, huolto- ja käyttötoimintaa voidaan ulkoistaa, on tehtävä sitä koskeva riskien arviointi ja osoitettava, että jäännösriski on hyväksyttävällä tasolla. **[**2021-02-12 **]**

322. Tietoturvallisuuden kouluttamiseen, kehittämiseen ja ylläpitoon osallistuvien henkilöiden koulutus ja osaamisen ylläpito on oltava riittävää heidän tehtäviensä toteuttamiseksi. **[**2021-02-12 **]**

322a. Ydinlaitoksen koko henkilökunnan sekä ulkoisten resurssien on oltava tietoisia tietoturvallisuuden hallintaan liittyvistä asioista tehtäviensä hoitamisen kannalta. **[**2021-02-12 **]**

322b. Tietoturvakoulutuksista on ylläpidettävä osallistujarekisteriä. **[**2021-02-12 **]**

323. Ulkoisten resurssien käytön osalta luvanhaltijan on huolehdittava, että niiden tietoturvallisuuden taso ja vastuujärjestelyt ovat vähintään samalla tasolla kuin luvanhaltijalla vastaavissa toimissa. **[**2021-02-12 **]**

323a. Luvanhaltijalla on oltava menettelyt, joilla se valvoo ulkoisten resurssien tietoturvallisuutta. Valvonnassa on huomioitava alihankintaketjut. Ohjeissa YVL A.3 ”Turvallisuuden johtaminen ydinalalla” ja YVL A.5 ”Ydinlaitoksen rakentaminen ja käyttöönotto” on esitetty vaatimuksia toimittajien valvonnalle. **[**2021-02-12 **]**

3.4 Tietoturvallisuuden hallintajärjestelmän arvioinnit, tarkastukset ja katselmoinnit

324. Luvanhaltijan on järjestettävä tietoturvallisuuden hallintajärjestelmän itsearviointi vuosittain siten, että kaikki osa-alueet arvioidaan vähintään kolmen vuoden välein. Hallintajärjestelmän toimivuuden ja riittävyyden arvioinnissa on huomioitava myös riskien arviointiin ja uhkakuvaan tulleet muutokset ja ajanjaksolla ilmenneet tietoturvallisuustapahtumat. **[**2021-02-12 **]**

325. Luvanhaltijan on erikseen kokoon kutsutun, luvanhaltijan toiminnasta riippumattoman asiantuntijaryhmän avulla toteutettava laaja-alainen tietoturvallisuuden arviointi määräajoin, kuitenkin vähintään neljän vuoden välein. **[**2021-02-12 **]**

326. Itsearvioinneista, riippumattoman asiantuntijaryhmän ja mahdollisten ulkoisten resurssien toteuttamista arvioinneista, tarkastuksista ja katselmoinneista on ilmoitettava riittävän ajoissa etukäteen STUKille, jotta STUK voi harkintansa mukaan seurata näiden toteuttamista. **[**2013-11-22 **]**

327. Poikkeamia arvioitaessa on kiinnitettävä huomiota toistuviin havaintoihin ja poikkeamiin. Sellaisten perussyyt on arvioitava ja korjaavat sekä ennaltaehkäisevät toimet on toteutettava siten, että toistuvat poikkeamat saadaan hallintaan. **[**2013-11-22 **]**

328. Poistettu. **[**2021-02-12 **]**

329. Tarkastukset, arvioinnit ja katselmoinnit sekä niiden tulokset on dokumentoitava. **[**2021-02-12 **]**

3.5 Tietoturvallisuuden hallintajärjestelmän parantaminen

330. Jatkuvassa parantamisessa on hyödynnettävä arviointien, tarkastusten, katselmointien ja harjoitusten tuloksia sekä oman ja muiden toimialojen tietoturvallisuuden hallinnasta saatuja käyttökokemuksia. **[**2021-02-12 **]**

331. Johdon on edistettävä tapoja, joilla koko henkilökunta osallistuu tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja jatkuvaan parantamiseen. **[**2021-02-12 **]**

332. Luvanhaltijan johdon on varmistettava, että tietoturvallisuuden hallintajärjestelmään kohdistuvat parannukset ovat asetettujen tavoitteiden mukaisia. **[**2021-02-12 **]**

4 Turvallisuuden kannalta tärkeiden järjestelmien suojaaminen

401. Poistettu. **[**2021-02-12 **]**

4.1 Yleiset vaatimukset

402. Ydinlaitoksen turvallisuuteen suoraan tai välillisesti vaikuttavien laitteiden ja järjestelmien tietoturvallisuus ja arkkitehtuuri on suunniteltava ja toteutettava siten, että luvaton pääsy on estetty tietoturvallisuuden hallintakeinojen ja turvajärjestelyjen avulla niin hyvin kuin käytännöllisin toimenpitein on mahdollista. **[**2021-02-12 **]**

402a. Tietoturvallisuus on huomioitava ydinlaitoksen elinkaaren kaikissa vaiheissa, myös myöhemmin laitosta koskevien perusparannusten ja muutostöiden yhteydessä. Määritellyt hallintakeinot tulee olla käytössä ja niitä täytyy valvoa, katselmoida ja tarvittaessa parantaa. **[**2021-02-12 **]**

403. Luvattomien laitteiden asentaminen on estettävä koko elinkaaren ajan. **[**2021-02-12 **]**

403a. Luvattomien ohjelmien asentaminen on estettävä koko elinkaaren ajan. **[**2021-02-12 **]**

403b. Käynnit sähkö- ja automaatiojärjestelmiin sekä -laitteisiin ja käyntien aikana tehdyt muutokset ohjelmistoihin ja parametreihin on voitava jäljittää. **[**2021-02-12 **]**

404. Tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmät, verkottuneet laitteet ja erillisjärjestelmät sekä turvavalvontajärjestelmät ja valmiustoiminnan viestintäjärjestelmät on suojattava. **[**2021-02-12 **]**

404a. Tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmiä, verkottuneita laitteita ja erillisjärjestelmiä sekä turvavalvontajärjestelmiä ja valmiustoiminnan viestintäjärjestelmiä koskevat asiakirjat ja tiedot on niiden turvallisuusmerkityksen mukaisesti suojattava siten, että vain henkilöt, joilla on oikeus niiden käsittelyyn, voivat saada ne haltuunsa. **[**2021-02-12 **]**

404b. Ohjeen YVL B.1 luvun 6.2 tarkoittamien järjestelmämuutosten ja ohjeen YVL A.5 tarkoittamien laitosmuutosten yhteydessä laitos- ja järjestelmätason tietoturvavaatimukset on arvioitava uudelleen. Arvioinnin on katettava myös uusittavaan järjestelmään yhteydessä olevat järjestelmät ja rajapinnat. **[**2021-02-12 **]**

405. Verkottuneet laitteet kattavat kaikki ne laitteet, jotka on liitetty toiseen laitteeseen tietoliikenteen mahdollistavalla tavalla. Näihin liittyvä tietoliikenne ja fyysinen kaapelointi on suojattava luvattomalta toiminnalta. **[**2021-02-12 **]**

405a. Verkkojen fyysinen ja looginen erottelu on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen. **[**2021-02-12 **]**

405b. Verkkojen tietoliikenteen valvonta on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen. **[**2021-02-12 **]**

405c. Ohjeen YVL E.7 tarkoittamiin ydinturvallisuuden kannalta keskeisiin ohjelmistopohjaisiin järjestelmiin ei saa olla fyysistä mahdollisuutta muodostaa järjestelmään kuulumatonta tiedonsiirtoyhteyttä järjestelmän ulkopuolelta sisäänpäin. **[**2021-02-12 **]**

405d. Ohjeen YVL B.1 luvun 5.2.5 tarkoittama suojausautomaatio on erotettava toiminnallisesti muista automaatiojärjestelmistä siten, että verkotettu tiedonsiirto on estetty suojausautomaatioon päin käyttäen fyysisesti yhdensuuntaistavaa erotinta. **[**2021-02-12 **]**

405e. Automaatioarkkitehtuurin ja hallinnollisten tietojärjestelmien välinen rajapinta on toteutettava yhdensuuntaistamalla tiedonsiirto siten, että tiedonsiirto on estetty automaatioarkkitehtuuriin päin käyttäen fyysisesti yhdensuuntaistavaa erotinta. **[**2021-02-12 **]**

405f. Ohjelmistopohjainen tiedonsiirron yksisuuntaisuuden järjestäminen ei ole riittävä suojautumiskeino toteuttamaan vaatimuksia 405c, 405d ja 405e. **[**2021-02-12 **]**

405g. Verkottuneiden järjestelmien osalta on kuvattava kattavasti ja yksiselitteisesti eri järjestelmien rajapinnat, yhteydet, käytetyt protokollat sekä kommunikoivat osapuolet. **[**2021-02-12 **]**

405h. Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä. **[**2021-02-12 **]**

406. Yksittäisen henkilön mahdollisuutta asentaa haitallinen toiminnallisuus useisiin rinnakkaisiin, samaa turvallisuustoimintoa suorittaviin laitteisiin tai järjestelmiin on rajoitettava. **[**2021-02-12 **]**

406a. Yksittäisen ohjelmiston haitallinen vaikutus ydinlaitoksen turvallisuuteen on tehtävä niin pieneksi kuin käytännöllisin keinoin on mahdollista. **[**2021-02-12 **]**

406b. Haitallisen toiminnallisuuden asentaminen tai suojaustoiminnon lamauttaminen on voitava havaita luotettavasti. **[**2021-02-12 **]**

407. Siirretty numerolle 404a. **[**2021-02-12 **]**

408. Poistettu. **[**2021-02-12 **]**

409. Poistettu. **[**2021-02-12 **]**

410. Poistettu. **[**2021-02-12 **]**

411. Poistettu. **[**2021-02-12 **]**

412. Poistettu. **[**2021-02-12 **]**

413. Siirretty numerolle 405g. **[**2021-02-12 **]**

414. Siirretty numerolle 405h. **[**2021-02-12 **]**

4.2 Tietoturvallisuustapahtumien hallinta

415. Tietoturvallisuuden hallintajärjestelmässä on oltava menettelyt tietoturvallisuuspoikkeamien havaitsemiseen, tunnistamiseen ja käsittelyyn. Hallintajärjestelmässä on oltava menettelyt vahingollisten seurausten estämiseksi ja rajoittamiseksi. **[**2021-02-12 **]**

415a. Tietoturvallisuuspoikkeamien havaitsemista ja hallintaa on harjoiteltava. Harjoituksista on informoitava STUKia etukäteen. **[**2021-02-12 **]**

416. Poistettu. **[**2021-02-12 **]**

417. Tietoturvallisuuspoikkeamien ilmoittamiseen on luotava menettelyt. STUKille on ilmoitettava kaikki turvallisuuden kannalta merkittävät tietoturvallisuuspoikkeamat viipymättä. **[**2021-02-12 **]**

417a. Kaikista laitoksen todetuista tietoturvallisuutta koskevista ja niihin liittyvistä uhkista, tapahtumista ja ilmiöistä, joilla saattaa olla merkitystä ydinturvallisuuden kannalta tai jotka voivat ylittää kansallisen tai kansainvälisen uutiskynnyksen, on ilmoitettava mahdollisimman pian STUKille. **[**2021-02-12 **]**

4.3 Käyttöoikeuksien hallinta

418. Käyttöoikeuksien hallintaperiaatteet on laadittava, dokumentoitava ja katselmoitava. **[**2021-02-12 **]**

418a. Käyttäjien käyttöoikeudet on katselmoitava säännöllisesti ja työtehtävien muutosten yhteydessä. **[**2021-02-12 **]**

418b. Salasanapolitiikka on oltava käytössä, ja sen toteutumista on valvottava. **[**2021-02-12 **]**

419. Pääkäyttäjäoikeuksia on rajoitettava järjestelmäkohtaisesti. Käyttöoikeudet on myönnettävä vain työtehtävien mukaisesti. **[**2021-02-12 **]**

419a. Pääsyä suojattaviin kohteisiin on hallittava ja valvottava pääsynhallinta- ja lokimenettelyin. Lokimerkintöjen tulee sisältää riittävät tiedot tapahtuman ja käyttäjän jäljittämiseen. **[**2021-02-12 **]**

419b. Lokitiedostot on suojattava luvattomilta muutoksilta. **[**2021-02-12 **]**

420. Siirretty numerolle 418a. **[**2021-02-12 **]**

421. Siirretty numerolle 418b. **[**2021-02-12 **]**

422. Poistettu. **[**2021-02-12 **]**

4.4 Järjestelmien turvallisuustestaaminen

423. Turvavalvontajärjestelmien tietoturvallisuus on testattava. Turvallisuustestausta voidaan suorittaa myös ohjeen YVL A.11 edellyttämien turvajärjestelyjen vaikuttavuuden osoittamiseksi järjestettävien harjoituksien yhteydessä. **[**2021-02-12 **]**

424. Ohjeen YVL E.7 tarkoittamien automaatiojärjestelmäalustojen, sähkö- ja automaatiolaitteiden ja -järjestelmien kelpoistuksessa ja testaamisessa on huomioitava myös tietoturvallisuus. **[**2021-02-12 **]**

425. Automaatioarkkitehtuuriin liittyvien verkkojen, erityisesti laitosverkkojen, testaamisessa on käytettävä kehittyneitä menettelyjä. **[**2021-02-12 **]**

426. Poistettu. **[**2021-02-12 **]**

5 Säteilyturvakeskuksen valvontaa varten toimitettavat asiakirjat

5.1 Periaatepäätösvaihe

501. Ydinenergia-asetuksen (161/1988) [15] 24 §:n mukaisesti ydinlaitoksen periaatepäätöstä koskevaan hakemukseen on liitettävä selvitys suunnitellun sijaintipaikan sopivuudesta tarkoitukseensa ottaen huomioon paikallisten olosuhteiden vaikutus turvajärjestelyihin.
[2021-02-12 **]**

5.2 Rakentamislupavaihe

502. Rakentamislupahakemuksen yhteydessä on toimitettava seuraavat asiakirjat STUKille hyväksyttäväksi:

1. vaatimuksen 308 mukainen luvanhakijan tietoturvallisuuden hallintapolitiikka ja luvun 3.1 mukaisen tietoturvallisuuden hallintajärjestelmän kuvaus, josta saadaan kokonaisvaltainen käsitys tietoturvallisuuden ja tietoturvariskien hallinnasta
2. laitostason suunnittelun tietoturvavaatimukset
3. arkkitehtuuritason tietoturvasuunnitelmat, mukaan lukien kuvaus järjestelmien välisistä yhteyksistä.

[2021-02-12 **]**

503. Seuraavat asiakirjat on toimitettava STUKille tiedoksi:

1. asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittyvät menettelyt
2. järjestelmäkohtaiset tietoturvavaatimukset
3. vaatimuksen 310 mukainen kuvaus rakentamisen aikaisesta tietoturvaorganisaatiosta
4. vaatimuksen 323a mukaisesti suunnitelma ydinlaitoksen rakentamisen aikaisista toimittajiin kohdistuvista tietoturvallisuuden valvontatoimista.

[2021-02-12 **]**

504. Poistettu. **[**2021-02-12 **]**

505. Poistettu. **[**2021-02-12 **]**

5.3 Rakentamisvaihe

506. Ydinlaitoksen rakentamisen aikana STUKin hyväksyttäväksi on toimitettava seuraavat asiakirjat:

1. vaatimuksen 502 asiakirjojen merkittävät muutokset
2. luvun 4.4 mukaiset järjestelmäalusta-, järjestelmä- tai laitekohtaiset turvallisuustestaussuunnitelmat.

[2021-02-12 **]**

507. Seuraavat asiakirjat ja niiden päivitykset on toimitettava STUKille tiedoksi:

1. vaatimuksen 503 asiakirjojen merkittävät muutokset
2. luvun 4.4 mukaiset turvallisuustestien raportit.

[2021-02-12 **]**

508. Poistettu. **[**2021-02-12 **]**

509. Poistettu. **[**2021-02-12 **]**

5.4 Käyttölupavaihe

510. Poistettu. **[**2021-02-12 **]**

511. Käyttölupahakemuksen käsittelyä varten on STUKille toimitettava rakentamislupa- ja rakentamisvaiheen asiakirjat lopullisessa muodossaan sekä muut STUKin vaatimat asiakirjat ja selvitykset, joilla voidaan todentaa tietoturvallisuuden riittävä taso. Käyttölupahakemuksen käsittelyä varten tarvittavat asiakirjat ovat

1. käytön aikaisen tietoturvallisuuden hallintajärjestelmän kuvaus
2. analyysi tietoturvavaatimusten täyttymisestä laitos-, arkkitehtuuri- ja järjestelmätasolla
3. kuvaus käyttövaiheen tietoturvaorganisaatiosta.

[2021-02-12 **]**

5.5 Käyttövaihe

512. Käyttövaiheessa STUKille on toimitettava tiedoksi

1. laitos- tai järjestelmämuutosten yhteydessä vaatimuksen 404b tarkoittama arvio ja päivitetyt vaatimukset
2. vaatimuksen 511 mukaisten asiakirjojen päivitykset.

[2021-02-12 **]**

513. Poistettu. **[**2021-02-12 **]**

514. Poistettu. **[**2021-02-12 **]**

5.6 Käytöstäpoistovaihe

515. Luvanhaltijan on toimitettava STUKille hyväksyttäväksi selvitys menettelyistä, joilla tietoturvallisuus toteutetaan käytöstäpoistovaiheen aikana ennen käytöstäpoistotoimien aloittamista. **[**2013-11-22 **]**

6 Säteilyturvakeskuksen valvontamenettelyt

6.1 Periaatepäätösvaihe

601. Ydinenergia-asetuksen 25 §:n mukaisesti Säteilyturvakeskuksen on liitettävä periaatepäätöshakemuksesta antamaansa alustavaan turvallisuusarvioon ydinenergialain 56 §:n 2 momentissa tarkoitetun neuvottelukunnan lausunto. **[**2021-02-12 **]**

6.2 Rakentamislupavaihe

602. Rakentamislupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja ydinenergia-asetuksen 35 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuusarviota valmistellessaan STUK pyytää sisäministeriöltä lausunnon ydinenergia-asetuksen 35 §:n 1 momentin kohdassa 6 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä. **[**2021-02-12 **]**

603. STUK todentaa luvussa 5.2 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**2021-02-12 **]**

604. Rakentamislupahakemuksen käsittelyn aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**2013-11-22 **]**

605. Rakentamislupahakemuksen käsittelyn aikana STUK voi osallistua harkintansa mukaan tietoturvallisuuden tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**2021-02-12 **]**

605a. STUK tarkastaa luvanhakijan osoittamassa paikassa vaatimuksen 314 mukaiset tietoturvallisuuden uhka- ja riskiarvioinnin tulokset. **[**2021-02-12 **]**

6.3 Rakentamisvaihe

606. STUK todentaa luvussa 5.3 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**2021-02-12 **]**

607. Rakentamisen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**2013-11-22 **]**

608. STUK voi osallistua harkintansa mukaan rakentamisen aikaisiin tietoturvallisuuden tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**2021-02-12 **]**

608a. STUK tarkastaa rakennusluvanhaltijan osoittamassa paikassa vaatimuksen 323a mukaiset raportit valvontatoimista, vaatimuksen 324 mukaiset arviointiraportit sekä vaatimuksen 325 mukaiset arviointiraportit. **[**2021-02-12 **]**

6.4 Käyttölupavaihe

609. Käyttölupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja ydinenergia-asetuksen 36 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuuden kokonaisarviota valmistellessaan STUK käsittelee myös tietoturvallisuuden hallintaa ja pyytää sisäministeriöltä lausunnon ydinenergia-asetuksen 36 §:n 1 momentin 7 kohdassa tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä. **[**2021-02-12 **]**

610. STUK todentaa luvussa 5.4 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**2013-11-22 **]**

611. Käyttölupavaiheen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**2013-11-22 **]**

611a. STUK tarkastaa luvanhakijan osoittamassa paikassa vaatimuksen 314 mukaisen käytön aikaisen tietoturvallisuuden uhka- ja riskiarvioinnin tulokset. **[**2021-02-12 **]**

6.5 Käyttövaihe

612. STUK todentaa luvussa 5.5 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**2021-02-12 **]**

613. Käytön aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**2021-02-12 **]**

614. STUK voi osallistua harkintansa mukaan käytön aikaisiin tietoturvallisuuden tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**2021-02-12 **]**

615. STUK valvoo tietoturvallisuuden hallintajärjestelmän toimintoja osana käytön valvonnan tarkastusohjelmaa. Lisäksi STUK tekee muita tarkastuksia harkintansa mukaan. Tarkastukset voivat kohdistua luvanhaltijaan tai luvanhaltijan käyttämään toimittajaan. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**2021-02-12 **]**

615a. STUK tarkastaa luvanhaltijan osoittamassa paikassa vaatimuksen 323a mukaiset raportit valvontatoimista, vaatimuksen 324 mukaiset arviointiraportit, vaatimuksen 325 mukaiset arviointiraportit sekä ajantasaiset, vaatimuksen 314 mukaiset tietoturvallisuuden uhka- ja riskiarvioinnin tulokset. **[**2021-02-12 **]**

6.6 Käytöstäpoistovaihe

616. STUK valvoo käytöstäpoistovaiheessa suojattavien tietojen käsittelyä harkintansa mukaan. **[**2021-02-12 **]**

617. Poistettu. **[**2021-02-12 **]**

618. Poistettu. **[**2021-02-12 **]**

7 Viitteet

1. Ydinenergialaki (990/1987). **[**2013-11-22 **]**

2. Säteilyturvakeskuksen määräys ydinenergian käytön turvajärjestelyistä (STUK Y/3/2020). **[**2021-02-12 **]**

3. Säteilyturvakeskuksen määräys ydinvoimalaitoksen turvallisuudesta (STUK Y/1/2018). **[**2021-02-12 **]**

4. Laki viranomaisten toiminnan julkisuudesta (621/1999). **[**2013-11-22 **]**

5. Poistettu. **[**2021-02-12 **]**

6. Poistettu. **[**2021-02-12 **]**

7. Poistettu. **[**2021-02-12 **]**

8. Poistettu. **[**2021-02-12 **]**

9. VAHTI-ohjeistus, www.vahtiohje.fi. **[**2021-02-12 **]**

10. Poistettu. **[**2021-02-12 **]**

11. Poistettu. **[**2021-02-12 **]**

12. Poistettu. **[**2021-02-12 **]**

13. KATAKRI, kansallinen turvallisuusauditointikriteeristö (2020). **[**2021-02-12 **]**

14. Poistettu. **[**2021-02-12 **]**

15. Ydinenergia-asetus (161/1988). **[**2013-11-22 **]**

16. Poistettu. **[**2021-02-12 **]**

17. Poistettu. **[**2021-02-12 **]**

18. Poistettu. **[**2021-02-12 **]**

19. SFS-EN ISO/IEC 27000. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. **[**2021-02-12 **]**

20. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). **[**2021-02-12 **]**

21. Neuvoston päätös, annettu 23 päivänä syyskuuta 2013, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). **[**2021-02-12 **]**

Määritelmät

Järjestelmä (tietoturvallisuuteen liittyvä) (system (information security))
Tietoturvallisuuteen liittyvällä järjestelmällä tarkoitetaan tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Järjestelmä voi olla esimerkiksi tieto-, tietoliikenne-, sähkö- tai automaatiojärjestelmä tai turvavalvonnan ja valmiustoiminnan viestintäjärjestelmä.

Riskianalyysi (risk analysis)
Riskianalyysillä tarkoitetaan järjestelmällisin menetelmin tehtäviä selvityksiä, joilla 1) kartoitetaan uhkat, ongelmat ja haavoittuvuudet, 2) tunnistetaan näihin johtavat syyt sekä 3) arvioidaan ja luokitellaan ei-toivottujen tilanteiden seuraukset ja niihin liittyvät riskit. (STUK Y/3/2020)

Tietoturvallisuuden hallintajärjestelmä (information security management system)
Tietoturvallisuuden hallintajärjestelmä koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista tai toiminnoista joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan.

Turvajärjestelyt (nuclear security)
Turvajärjestelyillä tarkoitetaan ydinenergian käytön turvaamiseksi ydin- tai säteilyturvallisuutta vaarantavalta toiminnalta tarvittavia toimenpiteitä ydinlaitoksessa, sen alueella, muussa paikassa tai kulkuvälineessä, jossa ydinenergian käyttöä harjoitetaan. (YEL 990/1987)