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 dd.mm.2019 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/3/2016) säädettyjä suunnitteluvaatimuksia. Määräyksen 4 §:n mukaan ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa ja ylläpidossa on käytettävä kehittyneitä, tarkoituksenmukaisia tietoturvallisuusperiaatteita. Turvallisuuden kannalta tärkeitä järjestelmiä koskevan luvattoman toiminnan ja tietoturvallisuuspoikkeamien havaitsemiksi ja estämiseksi sekä vahingollisten seurausten rajoittamiseksi on oltava tehokkaat menetelmät. Määräyksen 5 §:n mukaan ydinlaitoksella on varauduttava tietoturvallisuusuhkista johtuvien poikkeavien tilanteiden hallintaan. **[**Muutos säädösviittaukseen, VNA 734/2008 korvattu STUK Y/3/2016 **]**

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) 78 §:ssä [1]. **[**Selkeytys ja pieni muutos, Poistettu jälkimmäinen lause, koska YEL määrittelee suojattavat tiedot. Lisätty velvollisuus suojata tietoa YEL mukaisesti. **]**

103. Turvajärjestelyjä koskevat yleiset velvoitteet esitetään ydinenergialaissa (990/1987) [1] ja sen nojalla annetuissa Säteilyturvakeskuksen määräyksissä STUK Y/3/2016 [2] ja 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 [1]. **[**Muutos säädösviittaukseen, Korvattu VNA määräyksillä STUK Y/3/2016 ja STUK Y/1/2018 **]**

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

turvajärjestelyjä. **[**Selkeytys ja pieni muutos, Poistettu tietoturvamenettelyjen jaottelu tästä kohdasta, koska jaottelua on poistettu myös muualta ohjeesta. **]**

105. Tietoturvallisuus kattaa tiedon eheyden, käytettävyyden ja luottamuksellisuuden turvaamisen sen kaikissa olomuodoissaan aina tiedon luomisesta sen tuhoamiseen asti. **[**Selkeytys ja pieni muutos, Aikaisemmin termejä tieto ja asiakirja oli käytetty ristiin. Päivitetyssä ohjeessa käytetään termiä tieto, ellei nimenomaisesti puhuta tietystä asiakirjasta. **]**

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 lukua 3, pois lukien vaatimukset 324, 325 ja 326. Tietoturvallisuuden kannalta tärkeitä vaatimuksia ja STUKin suorittamaa valvontaa kuvataan myös YVL A-sarjan 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
- D.1 Ydinmateriaalivalvonta
- D.2 Ydinaineiden ja ydinjätteiden kuljetus
- D.3 Ydinpolttoaineen käsittely ja varastointi
- D.5 Ydinjätteiden loppusijoitus
- E.7 Ydinlaitoksen sähkö- ja automaatiolaitteet

[Merkittävä muutos sisältöön, Tietoturvallisuuden kannalta tärkeitä vaatimuksia kuvataan luettelossa mainituissa ohjeissa. Korjattu kohta, jossa määritellään, mitkä vaatimukset koskevat muuta ydinenergian käyttöä. Selvennetty, että ohje koskee sekä luvanhaltijaa että -hakijaa. **]**

3 Tietoturvallisuuden hallinta

3.1 Tietoturvallisuuden hallintajärjestelmä

301. Luvanhaltijan johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintaan. **[**Selkeytys ja pieni muutos, Vaatimus selvennettiin koskemaan luvanhaltijaa, kuten luvun muutkin vaatimukset koskevat. **]**

302. Luvanhaltijalla on oltava tietoturvallisuuden hallintajärjestelmä, joka on osa johtamisjärjestelmää. **[**Selkeytys ja pieni muutos, Lisätty luvanhakija ja muokattu tekstiä, jaettu. **]**

303. *Tietoturvallisuuden hallintajärjestelmä koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä resursseista tai toiminnoista joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan*. [19] **[**Selkeytys ja pieni muutos, Jaettu, Korvattu aikasempi teksti ISO/IEC 27000 -määritelmällä. Ulkoiset resurssit on jaettu vaatimukseen 303b. **]**

303a. Tietoturvallisuuden hallintajärjestelmän on katettava toimenpiteet ja menettelyt, valita, toteuttaa ja parantaa asianmukaisia hallintakeinoja. **[**Selkeytys ja pieni muutos, 303 määrittelyä on jatkettu, jotta se olisi yhdenmukainen ISO/IEC 27000 kanssa. **]**

303b. Tietoturvallisuuden hallintajärjestelmän on katettava ulkoisten resurssien ohjaaminen ja valvonta tietoturvallisuuden osalta. **[**Jaettu, hallinnollinen tietoturva 303 tekninen tietoturva 303a 303b resurssien ohjaaminen ja valvonta **]**

304. Kansainväliset tietoturvallisuuden standardit ja ohjeistukset [5–8, 12, 14, 18, 19] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 304 on jaettu, kansainväliset ohjeistukset vaatimuksessa 304 ja kansallliset ohjeistukset 304a. Viitelistassa on huomioitu nimenomaan ydinalaa koskevat ohjeet ja standardit. **]**

304a. Kansalliset ohjeistukset [9–11, 13] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 304 on jaettu, kansainväliset ohjeistukset vaatimuksessa 304 ja kansallliset ohjeistukset 304a. Viitelistassa on huomioitu nimenomaan ydinalaa koskevat ohjeet ja standardit. **]**

305. Ohje YVL A.11 esittää vaatimuksen tilannekuvan välittämisestä. Tilannekuvan välittämisessä on huomioitava tietoturvallisuus, siten ettei tietoturvallisuudesta huolehtiminen saa vaarantaa ajantasaisen tilannekuvan välittämistä. **[**Selkeytys ja pieni muutos, poistettu sana

kuitenkin **]**

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. **[**Muutos säädösviittaukseen, Selkeytys ja pieni muutos, VNA korvatty STUKin määräyksellä. Määräyksen pykälässä ei rajoituta luvanhaltijoihin tai -hakijoihin, vaan se koskee nimenomaan kaikkia organisaatioita. **]**

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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

308. Luvanhaltijan on määriteltävä tietoturvallisuuden hallintapolitiikka, joka voi olla itsenäinen asiakirja tai osa laajempaa kokonaisuutta. **[**Selkeytys ja pieni muutos, Osa vaatimuksesta on poistettu, koska se oli päällekkäinen vaatimuksen 302 kanssa. **]**

309. Tietoturvallisuuden tavoitteet on esitettävä osana tietoturvallisuuden hallintajärjestelmää. **[**Jaettu, Saman numeron alla oli useita vaatimuksia , nyt ne on jaettu omille numeroilleen. Vaatimus toteutussuunnitelmasta poistettu, tavoitteiden saavuttamiseksi voi olla perustettuna erillinen projekti, mutta se voi olla myös osa päivittäistä muuta toimintaa. **]**

309a. Tietoturvallisuustavoitteiden saavuttamista on seurattava ja tavoitteita on arvioitava jatkuvan parantamisen periaatetta noudattaen. **[**Selkeytys ja pieni muutos, Jaettu, Vaatimuksen 309 alla oli useita vaatimuksia, nyt ne on jaettu omille numeroilleen. **]**

310. Tietoturvallisuusorganisaatio on kuvattava tietoturvallisuuden hallintajärjestelmässä. Kuvauksessa on otettava huomioon myös ulkoiset toimijat ja näiden vastuut. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimuksessa 310 oli useita vaatimuksia, osa on siirretty 310a. **]**

310a. Tehtävät ja vastuualueet on tarpeen mukaan eriytettävä, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. **[**Jaettu, Vaatimus 310 jaettiin vaatimuksiin 310 ja 310a. Poistettu sana organisaatio, koska se rajoitti vaatimusta. **]**

311. POISTETTU. Luvanhaltijan on dokumentoitava, mitä kriteereitä ja standardeja hyödyntäen tietoturvallisuuden hallintajärjestelmä on toteutettu. **[**Jaettu, Poistettu, Alkuperäisessä 311 vaatimuksessa oli useampi vaatimus. 304 ja 304a kanssa päällekkäinen osa on poistettu, ja

tiedon suojaukseen liittyvä vaatimus on siirretty numerolle 311a. **]**

311a. Viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen on käytettävä [20] ja [21] mukaisia menettelyjä. Ohjeistusta saa esimerkiksi VAHTI-ohjeista [22] ja suojauksen tietoturvallisuuden arviointiin voidaan käyttää esimerkiksi KATAKRI-kriteeristöä [13]. **[**Jaettu, Muutos säädösviittaukseen, Merkittävä muutos sisältöön, Muutettu lause selkeämmäksi niin, että KATAKRIn käyttö ei ole pakollista. Muutoksen jälkeen YVL A.11 ja A.12 ovat yhdenmukaisia. Vaihdettu viitteet valtioneuvoston asetuksiin. **]**

311b. VNa 681/2010, 15§ mukaisesti *luokiteltuja asiakirjoja ei saa säilyttää tai muutoin käsitellä valtionhallinnon viranomaisen toimitilojen ulkopuolella, ellei viranomaisen luvasta, toimeksiannosta tai antamista ohjeista muuta johdu*. Ennen viranomaisen turvallisuusluokittelemaa, salassa pidettävää tai näistä johdettua tietoa sisältävän aineiston luovuttamista kolmannelle osapuolelle luvanhaltijalla tulee olla Säteilyturvakeskuksen hyväksyntä tiedon luovuttamiselle. **[**Jaettu, Selkeytys ja pieni muutos, Kirjoitettu vaatimus selkeämmäksi lisäämällä VNa-tekstiä sekä "Säteilyturvakeskus". **]**

312. Luvanhaltijalla on oltava menettelyt tietoturvallisuuden riskien arviointiin ja hallintaan. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus on jaettu 312 ja 312a, ja kirjoitettu yksinkertaisempaan muotoon. **]**

312a. Luvanhaltijan on varmistettava, että tietoturvallisuuden riskien arviointiin käytetyt menettelyt ovat riittävät ja merkittävät riskit on tunnistettu. **[**Jaettu, Selkeytys ja pieni muutos, [Muutoksen perustelut] **]**

313. POISTETTU. Riskienhallinnan kokonaisuus on dokumentoitava. **[**Poistettu, Vanha vaatimus oli liian yleinen ja epäselvä. Muut vaatimukset kattavat tämän. **]**

314. Luvanhaltijan on tehtävä tietoturvallisuuden uhka- ja riskienarviointi, ja se on päivitettävä säännöllisesti ja merkittävien tietoturvallisuutta koskevien tapahtumien, muutosten tai uusien uhkien ilmentyessä. **[**[Muutoksen tyyppi], "Vuosittain" vaihdettu "säännöllisesti". **]**

315. Tietoturvallisuuden uhkat ja riskit on systemaattisesti analysoitava, ja suojaavat toimenpiteet ja menetelmät on valittava analyysin perusteella. **[**Selkeytys ja pieni muutos, Vaatimus on kirjoitettu yksinkertaisemmin. **]**

316. Suojattavat kohteet on tunnistettava ja määriteltävä riittävän yksityiskohtaisesti. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 316 sisälsi useita vaatimuksia, joten se on jaettu vaatimuksiin 316, 316a ja 316b. **]**

316a. Suojattaviin kohteisiin liittyvät uhkat ja haavoittuvuudet sekä tietoturvallisuustapahtumien

aiheuttamat vaikutukset on arvioitava ja niiden perusteella on määriteltävä tarpeelliset suojaustoimenpiteet. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 316 sisälsi useita vaatimuksia, joten se on jaettu vaatimuksiin 316, 316a ja 316b. **]**

316b. Suojaustoimenpiteet on dokumentoitava. **[**Jaettu, Vaatimus 316 sisälsi useita vaatimuksia, joten se on jaettu vaatimuksiin 316, 316a ja 316b. **]**

317. SIIRRETTY. Pääsyä suojattaviin kohteisiin on valvottava lokimenettelyin. Lokimerkintöjen täytyy sisältää riittävät tiedot tapahtuman ja käyttäjän jäljittämiseen. Lokitiedostot on suojattava asiattomilta muutoksilta. **[**Siirretty, Siirretty loogisempaan paikkaan ja samalla jaettu kahteen osaan. Lokitus liittyy käyttöoikeuksiin. Uudet vaatimusnumerot 422a ja 422b. **]**

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". **[**Merkittävä muutos sisältöön, Vaatimus on muutettu kuvaukseksi ja siihen on lisätty viitattavien ohjeiden nimet. Poistettu sana luvanhaltija, koska kuvaus koskee myös muiden toimijoiden asiakirjoja. **]**

319. Tieto on luokiteltava sen tietoturvallisuus- ja turvallisuusmerkityksen mukaan. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 319 sisälsi useita vaatimuksia, ne on jaettu vaatimuksiin 319 ja 319a. **]**

319a. Tietoa on suojattava luokituksen mukaisesti luvattomalta käytöltä, muuttamiselta ja tuhoamiselta. Tiedon saatavuus luvalliselle käyttäjälle on turvattava. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 319 sisälsi useita vaatimuksia, ne on jaettu vaatimuksiin 319 ja 319a. **]**

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. **[**Jaettu, Selkeytys ja pieni muutos, Tekstiä hiukan selkeytetty ja alkuperäinen vaatimus jaettu. 320 resurssit, lisätty ohjeiden nimet. **]**

320a. Luvanhaltijan on huolehdittava siitä, että sillä on käytettävissään riittävät resurssit ja osaaminen tietoturvallisuuden hallinnan suunnitteluun, toteuttamiseen, arviointiin ja jatkuvaan parantamiseen. **[**Jaettu, Vaatimus 320 sisälsi useita vaatimuksia, ja jaettiin 320 ja 320a. **]**

321. Keskeisten tietoturvallisuuden hallintaan liittyvien henkilöiden ja muiden resurssien on

oltava luvanhaltijan palveluksessa tai omistuksessa. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus on jaettu kahtia. Vaatimus 321 koskee riittäviä resursseja. Vaatimus 321a koskee ulkoistamisenriskiarviota. Poistettu sana luvanhakija luvun 2 perusteella. **]**

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

322. Tietoturvallisuuden kouluttamiseen, kehittämiseen ja ylläpitoon osallistuvien henkilöiden koulutus ja osaamisen ylläpito on oltava riittävää heidän tehtäviensä toteuttamiseksi. **[**Jaettu, Vanha vaatimus 322 sisälsi useita vaatimuksia. Ne on jaettu vaatimuksiin 322, 322a ja 322b. **]**

322a. Ydinlaitoksen koko henkilökunnan sekä ulkoisten resurssien on oltava tietoisia tietoturvallisuuden hallintaan liittyvistä asioista tehtäviensä hoitamisen kannalta. **[**Jaettu, Selkeytys ja pieni muutos, Vanha vaatimus 322 sisälsi useita vaatimuksia. Ne on jaettu vaatimuksiin 322, 322a ja 322b. **]**

322b. Tietoturvakoulutuksista on ylläpidettävä osallistujarekisteriä. **[**Jaettu, Selkeytys ja pieni muutos, Vanha vaatimus 322 sisälsi useita vaatimuksia. Ne on jaettu vaatimuksiin 322, 322a ja 322b. **]**

323. Ulkoisten resurssien käytön osalta luvanhaltijan on huolehdittava, että niiden tietoturvallisuuden taso ja vastuujärjestelyt ovat vähintään samalla tasolla kuin luvanhaltijalla vastaavissa toimissa. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 323 on jaettu vaatimuksiin 323 ja 323a. **]**

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. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 323 on jaettu. Vaatimus 328:sta on siirretty viittaus ohjeiden YVL A3. ja A.5 vaatimuksiin toimittajien valvonnalle. **]**

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. **[**Selkeytys ja pieni muutos, Sanamuotoja korjailtu, jotta luettavuus paranee. Lisäksi yhdenmukaistettu vaatimusta YVL A.3:n kanssa. **]**

325. Luvanhaltijan on erikseen kokoon kutsutun, luvanhaltijan toiminnasta riippumattoman asiantuntijaryhmän avulla toteutettava laaja-alainen tietoturvallisuuden arviointi määräajoin, kuitenkin vähintään neljän vuoden välein. **[**Selkeytys ja pieni muutos, Korjattu oikeinkirjoitusta. **]**

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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

328. POISTETTU. Luvanhaltijan on tarkastettava ulkoisten resurssien tietoturvallisuus. Ulkoisten resurssien tarkastusten on katettava riittävässä määrin vastaavat toiminnot kuin luvanhaltijalla on. Ohjeissa YVL A.3 ja A.5 on esitetty vaatimuksia toimittajien valvonnalle. **[**Poistettu, Vaatimuksen sisältämä asia on siirretty vaatimukseen 323 selkeämmin kirjoitettuna. **]**

329. Tarkastukset, arvioinnit ja katselmoinnit sekä niiden tulokset on dokumentoitava. **[**Selkeytys ja pieni muutos, Lisätty vaatimukseen arvioinnit. Lisäksi kommenttien perusteella erikseen kirjoitettu, että myös tulokset on dokumentoitava, jotta ajatus säilyy käännöksissä. **]**

3.5 Tietoturvallisuuden hallintajärjestelmän parantaminen

330. Jatkuvassa parantamisessa on hyödynnettävä arviontien, tarkastusten, katselmointien ja harjoitusten tuloksia, sekä oman ja muiden toimialojen tietoturvallisuuden hallinnasta saatuja käyttökokemuksia. **[**Selkeytys ja pieni muutos, Aukikirjoitettu ISO9001 edellyttämiä syötteitä hallintajärjestelmän parantamiseen. **]**

331. Johdon on edistettävä tapoja, joilla koko henkilökunta osallistuu tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja jatkuvaan parantamiseen. **[**Merkittävä muutos sisältöön, Vaatimuksesta on poistettu sana luvanhaltija. Kaikkien organisaatioiden on osallistuttava hallintajärjestelmän toteuttamiseen, vrt. turvallisuuskulttuurivaatimus. **]**

332. Luvanhaltijan johdon on varmistettava, että tietoturvallisuuden hallintajärjestelmään kohdistuvat parannukset ovat asetettujen tavoitteiden mukaisia. **[**Selkeytys ja pieni muutos, Korjattu tekstiä niin, että kyse on nimenomaan tietoturvallisuuden hallintajärjestelmästä, eikä yleisestä. **]**

4 Turvallisuuden kannalta tärkeiden järjestelmien suojaaminen

401. POISTETTU. Säteilyturvakeskuksen määräyksen STUK Y/3/2016 4 §:n mukaisesti ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa ja ylläpidossa on käytettävä kehittyneitä,
tarkoituksenmukaisia tietoturvallisuusperiaatteita. **[**Poistettu, Kohta poistettu, ja tekstiä siirretty vaatimukseen 101. **]**

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. **[**Selkeytys ja pieni muutos, Selkeytettiin tekstiä ja lisättiin "laitteet" STUK in määräyksen mukaiseksi. Poistettiin esimerkkiluettelo, siirretään ehkä perustelumuistioon. Korjattu tähän "hallintakeinot", kuten muuallakin ohjeessa. **]**

402a. Tietoturva 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. **[**Uusi nimike, Vaatimus 410 ei täsmentänyt mitä järjestelmiä koskee. L1-kuulemisen jälkeen muokattiin vaatimus uusiksi. Selkeytetty, että kyse on nimenomaan ydinlaitoksen elinkaaresta. **]**

403. Luvattomien laitteiden asentaminen on estettävä koko elinkaaren ajan. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimuksessa oli kaksi asiaa, joten se on jaettu 403 ja 403a. 403.b on siirretty ohjeesta YVL E.7. Version L1 kuulemisen jälkeen korjattu sanamuotoja. **]**

403a. Luvattomien ohjelmien asentaminen on estettävä koko elinkaaren ajan. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimuksessa oli kaksi asiaa, joten se on jaettu 403 ja 403a. 403.b on siirretty ohjeesta YVL E.7. Version L1 kuulemisen jälkeen korjattu sanamuotoja. **]**

403b. (E.7 634.) Käynnit sähkö- ja automaatiojärjestelmiin sekä -laitteisiin ja käyntien aikana tehdyt muutokset ohjelmistoihin ja parametreihin on voitava jäljittää. **[**Siirretty, Selkeytys ja pieni muutos, Vaatimus on siirretty YVL ohjeesta E.7. Sanamuotoja on korjattu. **]**

404. Tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmät, verkottuneet laitteet ja erillisjärjestelmät sekä turvavalvontajärjestelmät ja valmiustoiminnan viestintäjärjestelmät on suojattava. **[**Selkeytys ja pieni muutos, Vaatimuksesta on poistettu viittaus A.11 vyöhykkeisiin, koska näiden vyöhykkeiden jako on pääosin liian karkea tietoturvan tarpeisiin. **]**

404a. (407) 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. **[**Siirretty, Siirretty kohdasta 407 luettavuuden parantamiseksi. **]**

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. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimuksessa oli useita vaatimuksia, ne on jaettu 405, 405a ja 405b. Poistettu maininta siitä, että verkottunut laite on nimenomaan kaapelilla kytketty. **]**

405a. Verkkojen fyysinen ja looginen erottelu on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen. **[**Jaettu, Vaatimuksessa 405 oli useita vaatimuksia, ne on jaettu 405, 405a ja 405b. **]**

405b. Verkkojen tietoliikenteen valvonta on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen.
[Jaettu, Vaatimuksessa oli useita vaatimuksia, ne on jaettu 405, 405a ja 405b. **]**

405c. (E.7 635.) Ohjeen YVL E.7 tarkoittamiin ydinturvallisuuden kannalta keskeisiin ohjelmistopohjaisiin järjestelmiin ei saa olla fyysistä mahdollisuutta muodostaa järjestelmään kuulumatonta tiedonsiirtoyhteyttä järjestelmän ulkopuolelta sisäänpäin. **[**Siirretty, Selkeytys ja pieni muutos, Vaatimus on siirretty ohjeesta YVL E.7. Vaatimusta on täsmennetty niin, että se ei kiellä esim. järjestelmän ylläpitoon tarvittavia yhteyksiä. **]**

405d. (B.1 5244.) 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. **[**Siirretty, Selkeytys ja pieni muutos, Vaatimus on siirretty ohjeesta B.1 ja sanamuotoa tarkennettu. **]**

405e. (B.1 5245.) Automaatioarkkitehtuurin ja hallinnollisten tietojärjestelmien välinen rajapinta on toteutettava yhdensuuntaistamalla tiedonsiirto siten, että tiedonsiirto on estetty automaatioarkkitehtuuriin päin käyttäen fyysisesti yhdensuuntaistavaa erotinta. **[**Siirretty, Selkeytys ja pieni muutos, Vaatimus on siirretty ohjeesta YVL B.1 ja sanamuotoa on tarkennettu. **]**

405f. (E.7 636.) Ohjelmistopohjainen tiedonsiirron yksisuuntaisuuden järjestäminen ei ole riittävä suojautumiskeino toteuttamaan vaatimuksia 405c, 405d ja 405e. **[**Siirretty, Selkeytys ja

pieni muutos, Vaatimus on siirretty ohjeesta YVL E.7 ja sitä on laajennettu. **]**

405g. (413.) Verkottuneiden järjestelmien osalta on kuvattava kattavasti ja yksiselitteisesti eri järjestelmien rajapinnat, yhteydet, käytetyt protokollat sekä kommunikoivat osapuolet. **[**Siirretty, Vaatimus koskee kaikkia järjestelmiä eikä pelkästään hankittuja, joten luku 4.1. on sille oikeampi paikka. **]**

405h. (414.) Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä. **[**Siirretty, Vaatimus koskee kaikkia järjestelmiä eikä pelkästään hankittuja, joten luku 4.1. on sille oikeampi paikka. **]**

406. Yksittäisen henkilön mahdollisuutta asentaa haitallinen toiminnallisuus useisiin rinnakkaisiin samaa turvallisuustoimintoa suorittaviin laitteisiin tai järjestelmiin on rajoitettava. **[**Jaettu, Selkeytys ja pieni muutos, Vaatimus 406 sisälsi useita vaatimuksia ja se on jaettu vaatimuksiin 406, 406a ja 406b. Poistettu sana luvanhaltija, koska vaatimus koskee muitakin, esimerkiksi laitostoimittajaa. **]**

406a. Yksittäisen ohjelmiston haitallinen vaikutus ydinlaitoksen turvallisuuteen on tehtävä niin pieneksi kuin käytännöllisin keinoin on mahdollista. **[**Jaettu, Vaatimus 406 sisälsi useita vaatimuksia ja se on jaettu vaatimuksiin 406, 406a ja 406b. Poistettu sana luvanhaltija, koska vaatimus koskee muitakin, esimerkiksi laitostoimittajaa. **]**

406b. Haitallisen toiminnallisuuden asentaminen tai suojaustoiminnon lamauttaminen on voitava havaita luotettavasti. **[**Jaettu, Vaatimus 406 sisälsi useita vaatimuksia ja se on jaettu vaatimuksiin 406, 406a ja 406b. Poistettu sana luvanhaltija, koska vaatimus koskee muitakin, esimerkiksi laitostoimittajaa. **]**

407. SIIRRETTY. 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. **[**Selkeytys ja pieni muutos, Poistettu L1-kuulemiseen, mutta kuulemiskommenttien perusteella vaatimus palautettiin takaisin. Järjestelmälistaa päivitetty vastaamaan vaatimusta 404. **]**

407a. 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. **[**Uusi nimike, Aikaisemmin ohje A.12 ei huomioinut selkeästi

laitosmuuksia. Nyt tietoturvan osalta on tarkennettu, mitä aineistoja STUKille on toimitettava. **]**

4.2 POISTETTU. Tietoliikenteen ja ICT-palveluiden hallinta ja kontrollointi

408. POISTETTU. Luvanhaltijalla on oltava kirjalliset menettelyohjeet turvallisille tietojenkäsittelypalveluille. **[**Poistettu, Poistettu kommenttien jälkeen, tietoturvallisuuden hallintajärjestelmän tulisi kattaa asia muutenkin. **]**

409. POISTETTU Konfiguraatiohallinnassa on huomioitava tietoturvallisuus. **[**Poistettu, Vaatimus on poistettu. YVL B.1 vaatimukset pitää täyttää joka tapauksessa ydinlaitoksien järjestelmien osalta. Hallinnollisen verkon puolella YVL B.1 vaatimuksia ei tarvitse täyttää. **]**

4.3 POISTETTU Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito

410. POISTETTU. Tietoturvallisuudesta tulee huolehtia tietoturvallisuuteen liittyvien järjestelmien kaikissa elinkaaren vaiheissa. **[**Poistettu, Vaatimusta selkeytettiin vanhasta ohjeesta L1-kuulemiseen. L1-kuulemisen perusteella tämä vaatimus poistettiin, ja kirjoitettiin kokonaan uusiksi numerolle 402.a. **]**

411. POISTETTU. Järjestelmien hankintaan, kehitykseen ja ylläpitoon liittyvän tietoturvallisuusdokumentaation on oltava kattavaa ja ajantasaista. Dokumentaation on selkeästi liityttävä muuhun järjestelmädokumentaatioon. **[**Poistettu, Tätä ei ole tarpeen vaatia erikseen. **]**

412. POISTETTU. Järjestelmien ja niiden osakomponenttien väliset toiminnalliset riippuvuudet on tunnistettava ja niiden vaikutus tietoturvallisuuteen on analysoitava ja arvioitava sekä poistettava haitalliset riippuvuudet. **[**Poistettu, Toiminnallisten riippuvuuksien analysointia vaaditaan jo YVL B.1. Haitallisia toimintoja koskee YVL E.7 vaatimus 517. **]**

413. SIIRRETTY Verkottuneiden järjestelmien osalta on kuvattava kattavasti ja yksiselitteisesti eri järjestelmien rajapinnat, yhteydet, käytetyt protokollat sekä kommunikoivat osapuolet. **[**Siirretty, Siirretty vaatimukseksi 405g. **]**

414. SIIRRETTY Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä. **[**Siirretty, Siirretty 405h. **]**

4.4 Tietoturvallisuustapahtumien hallinta

415. Tietoturvallisuuden hallintajärjestelmässä on oltava menettelyt tietoturvallisuuspoikkeamien havaitsemiseen, tunnistamiseen ja käsittelyyn. Hallintajärjestelmässä on oltava menettelyt vahingollisten seurausten estämiseksi ja rajoittamiseksi. **[**Merkittävä muutos sisältöön, Tekstiä selkeytetty. Lisätty vaatimus seurausten rajoittamisesta. Ilmoitusvelvollisuus on vaatimuksessa 417. **]**

415a. Tietoturvallisuuspoikkeamien havaitsemista ja hallintaa on harjoiteltava. Harjoituksista on informoitava STUKia etukäteen. **[**Uusi nimike, Lisätty uusi vaatimus harjoituksista. **]**

416. POISTETTU. Luvanhaltijan on luotava menettelyt järjestelmälliseen reagointiin tietoturvallisuuspoikkeamien varalta. **[**Poistettu, Vaatimuksen 415 muokkaamisen jälkeen vaatimus 416 oli sen kanssa päällekkäinen, joten se on poistettu. **]**

417. Tietoturvallisuuspoikkeamien ilmoittamiseen on luotava menettelyt. STUKille on ilmoitettava kaikki turvallisuuden kannalta merkittävät tietoturvallisuuspoikkeamat viipymättä. **[**Selkeytys ja pieni muutos, Viite ohjeeseen YVL A.3 on poistettu tarpeettomana. **]**

417a. Kaikista laitoksen todetuista tietoturvallisuutta koskevista ja niihin liittyvistä uhista, tapahtumista, ilmiöistä ja henkilöistä, joilla saattaa olla merkitystä ydinturvallisuuden kannalta tai jotka voivat ylittää kansallisen tai kansainvälisen uutiskynnyksen, on ilmoitettava mahdollisimman pian STUKille. **[**Uusi nimike, Lisätty vastaava tietoturvallisuutta koskeva vaatimus, kuin nykyisessä ohjeessa YVL A.11 on ollut jo pitkään. **]**

4.5 Käyttöoikeuksien hallinta

418. Käyttöoikeuksien hallintaperiaatteet on laadittava, dokumentoitava ja katselmoitava. **[**Selkeytys ja pieni muutos, Korvattu suppea "valvontaperiaatteet" laajemmalla "hallintaperiaatteilla" **]**

418a. (420.) Käyttäjien käyttöoikeudet on katselmoitava säännöllisesti ja työtehtävien muutosten yhteydessä. **[**Siirretty, Vaatimus 420. siirretty. **]**

418b. (421.) Salasanapolitiikka on oltava käytössä. Salasanapolitiikan toteutumista on valvottava. **[**Siirretty, Vaatimus 421 siirretty. **]**

419. Pääkäyttäjäoikeuksia on rajoitettava järjestelmäkohtaisesti. Käyttöoikeudet on myönnettävä vain työtehtävien mukaisesti. **[**Selkeytys ja pieni muutos, Selkiytetty tekstiä niin, että pääkäyttäjäoikeuksia on rajoitettava järjestelmäkohtaisesti. **]**

420. SIIRRETTY. Käyttäjien käyttöoikeudet on katselmoitava säännöllisesti ja työtehtävien muutosten yhteydessä. **[**Siirretty, Siirretty vaatimusnumerolle 418a. **]**

421. SIIRRETTY. Salasanapolitiikka on määriteltävä ja otettava käyttöön. Toteutumista on valvottava. **[**Siirretty, Siirretty vaatimusnumerolle 418b. **]**

422. POISTETTU. Etätyöhön ja ulkoisten resurssien tekemään työhön on luotava turvallisen tietojenkäsittelyn menettelyt ja näiden noudattamista on valvottava. **[**Poistettu, Ulkoisten resurssien valvonta on jo mainittu luvussa 3. Mahdollista etäyhteyttä koskevia vaatimuksia on annettu 405 alakohdissa. **]**

422a. (317.) Pääsyä suojattaviin kohteisiin on hallittava ja valvottava pääsynhallinta- ja lokimenettelyin. Lokimerkintöjen tulee sisältää riittävät tiedot tapahtuman ja käyttäjän jäljittämiseen. **[**Jaettu, Siirretty, Vanha 317 oli useampi vaatimus, siirretty ja jaettu kahtia numeroille 422a ja 422b. **]**

422b. Lokitiedostot on suojattava luvattomilta muutoksilta. **[**Jaettu, Vaatimuksen 317 osa on siirretty loogisempaan paikkaan, lokitus liittyy käyttöoikeuksiin. **]**

4.6 Järjestelmien turvallisuustestaaminen

423. Turvavalvontajärjestelmien tietoturvallisuus on testattava. Turvallisuustestausta voidaan suorittaa myös ohjeen YVL A.11 edellyttämien turvajärjestelyjen vaikuttavuuden osoittamiseksi järjestettävien harjoituksien yhteydessä. **[**Selkeytys ja pieni muutos, Korvattu "testattava tietoturvallisuuteen kohdistuvia hyökkäyksiä", tietoturva on testattava. Hyökkäys ei ole ainoa tietoturvariski. Termejä yhdenmukaistettu YVL A.11 kanssa. **]**

424. Ohjeen YVL E.7 tarkoittamien automaatiojärjestelmäalustojen, sähkö- ja automaatiolaitteiden ja järjestelmien kelpoistuksessa ja testaamisessa on huomioitava myös tietoturvallisuus. **[**Selkeytys ja pieni muutos, Lisätty automaatiojärjestelmäalustat selkeytyksen vuoksi **]**

425. Automaatioarkkitehtuuriin liittyvien verkkojen, erityisesti laitosverkkojen, testaamisessa on käytettävä kehittyneitä menettelyjä. **[**Selkeytys ja pieni muutos, Selkeytetty tekstiä ja poistettu päällekäisyyttä. Muutettu sanamuotoja niin, että alkuperäisen vaatimuksen eli testauksen rajaus tulee paremmin esille. **]**

426. POISTETTU. Erityistä huomiota on kiinnitettävä uusien ja mahdollisten vanhojen järjestelmien muodostaman kokonaisjärjestelmän tietoturvallisuuden arviointiin. **[**Poistettu, Siirretään perustelumuistioon, asia kuvattu luvussa 3.2 **]**

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 [16]. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

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.
3. Laitostason suunnittelun tietoturvavaatimukset.
4. Arkkitehtuuritason tietoturvasuunnitelmat, mukaan lukien kuvaus järjestelmien välisistä yhteyksistä.

Rakennuslupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja ydinenergia-asetuksen (161/1988) 35 §:n mukaisia asiakirjoja koskevan arvion, jossa käsitellään muun muassa suunniteltuja tietoturvallisuusjärjestelyjä. **[**Merkittävä muutos sisältöön, Tehty muutoksia toimitettaviin asiakirjoihin YVL B.1 pohjalta. Hallinnollista taakkaa kevennetty siirtämällä osa asiakirjoista tiedoksi toimitettaviin. Lisätty säädösviittaus YEA 1988/161 35§. Poistettu sana luvanhakija, jotta lause on yhdenmukainen muiden ohjeiden kanssa. **]**

503. Seuraavat asiakirjat on toimitettava STUKille tiedoksi:

1. Asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittyvät menettelyt.
2. Vaatimuksen 314 mukaisen tietoturvallisuuden uhka- ja riskiarvioinnin tulokset.
3. Järjestelmäkohtaiset tietoturvavaatimukset.
4. Vaatimuksen 310 mukainen kuvaus rakentamisen aikaisesta tietoturvallisuusorganisaatiosta.
5. Vaatimuksen 323a. mukaisesti suunnitelma ydinlaitoksen rakentamisen aikaisista toimittajiin kohdistuvista tietoturvallisuuden valvontatoimista. **[**Merkittävä muutos sisältöön, Analyysien tulokset ja organisaatiokuvaukset käsitellään tiedoksi tulleena. Korjattu yksittäisiä sanoja kommenttien perusteella. **]**

504. POISTETTU. Perustelluista syistä STUKille toimittamisen sijaan voidaan vaatimuksessa 503 esitetyt asiakirjat tarkastaa myös luvanhakijan osoittamassa paikassa. **[**Poistettu, Kyseessä ei ole vaatimus, vaan STUKin valvontamenettelyn kuvaus. Vastaavaa tekstiä ei ole muissakaan ohjeissa. **]**

505. POISTETTU. Vaatimuksissa 502 ja 503 esitetyt asiakirjat on päivitettävä rakentamisen aikana tehtävien muutosten yhteydessä. **[**Poistettu, YVL A.3 edellyttää jo asiakirjojen ajantasaisena pitämistä. **]**

5.3 Rakentamisvaihe

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

1. Vaatimuksen 502 asiakirjojen merkittävät muutokset.
2. Luvun 4.6 mukaiset järjestelmäalusta-, järjestelmä- tai laitekohtaiset turvallisuustestaussuunnitelmat. **[**Selkeytys ja pieni muutos, Selkiytetty asiakirjojen luetteloa. Poistettu riskiarvioinnin tulokset hyväksyttävistä asiakirjoista. **]**

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

1. vaatimuksen 503 asiakirjojen merkittävät muutokset
2. vaatimuksen 323a. mukaiset raportit valvontatoimista
3. vaatimuksen 324 mukaiset arviointiraportit.
4. vaatimuksen 325 mukainen arviointiraportti raportin valmistuttua
5. luvun 4.6 mukaiset turvallisuustestien raportit **[**Selkeytys ja pieni muutos, Muokattua toimitettavien asiakirjojen luetteloa ja lisätty niihin vaatimusten numerot luettavuuden parantamiseksi. **]**

508. POISTETTU. Perustelluista syistä vaatimuksessa 507 esitetyt asiakirjat voidaan STUKille toimittamisen sijasta todentaa myös rakentamisluvan hakijan osoittamassa paikassa. **[**Poistettu, Kyseessä ei ole vaatimus, vaan STUKin valvontamenettelyn kuvaus. Vastaavaa tekstiä ei ole muissakaan ohjeissa. **]**

509. POISTETTU. Vaatimuksissa 506 ja 507 esitetyt asiakirjat on pidettävä ajan tasalla. Edellä mainittujen asiakirjojen muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten edellä on mainittu. **[**Poistettu, YVL A.3 edellyttää jo asiakirjojen ajantasaisena pitämistä. **]**

5.4 Käyttölupavaihe

510. Käyttölupahakemuksen käsittelyn yhteydessä STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja ydinenergia-asetuksen (161/1988) 36 §:n mukaisia asiakirjoja koskevan arvion, jossa käsitellään muun muassa suunniteltuja tietoturvallisuusjärjestelyjä. Turvallisuusarviota valmistellessaan STUK pyytää sisäministeriöltä lausunnon YEA 36 §:n 1 momentin kohdassa 7 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15]. **[**Selkeytys ja pieni muutos, lisätty pilkku ja ministeriön nimi muutettu ajanmukaiseksi. **]**

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. Käytön aikaiset vaatimuksen 314 mukaisen tietoturvallisuuden uhka- ja riskiarvioinnin tulokset.
3. Analyysi tietoturvavaatimusten täyttymisestä laitos-, arkkitehtuuri- ja järjestelmätasolla.
4. Kuvaus käyttövaiheen tietoturvallisuusorganisaatiosta. **[**Selkeytys ja pieni muutos, Muokattu tekstiä, ja listattu käyttölupahakemuksen käsittelyä varten tarvittavat asiakirjat. **]**

5.5 Käyttövaihe

512. Käyttövaiheessa on toimitettava seuraavat asiakirjat ja näiden päivitykset STUKille hyväksyttäväksi:
1. Laitos- tai järjestelmämuutosten yhteydessä vaatimuksen 407a. tarkoittama arvio ja päivitetyt vaatimukset. **[**Merkittävä muutos sisältöön, Korjattu luvanhakija luvanhaltijaksi. Muokattu toimitettavien asiakirjojen luettelo. **]**

513. Seuraavat asiakirjat ja näiden päivitykset on toimitettava STUKille tiedoksi:
1. Vaatimuksen 511 mukaisten asiakirjojen päivitykset
2. Vaatimuksen 324 mukaiset arviointiraportit.
3. Vaatimuksen 325 mukaiset arviointiraportit. **[**Merkittävä muutos sisältöön, Toimitettavien asiakirjojen listaa on lyhennetty huomattavasti. **]**

514. POISTETTU. Perustelluista syistä tiedoksi toimitettavat asiakirjat tai vastaavat tiedot voidaan todentaa myös luvanhaltijan osoittamassa paikassa. **[**Poistettu, Kyseessä ei ole vaatimus, vaan STUKin valvontamenettelyn kuvaus. Vastaavaa tekstiä ei ole muissakaan

ohjeissa. **]**

5.6 Käytöstäpoistovaihe

515. Luvanhaltijan on toimitettava STUKille hyväksyttäväksi selvitys menettelyistä, joilla tietoturvallisuus toteutetaan käytöstäpoistovaiheen aikana ennen käytöstäpoistotoimien aloittamista. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

6 Säteilyturvakeskuksen valvontamenettelyt

6.1 Periaatepäätösvaihe

601. Ydinenergia-asetuksen (161/1988) [15] 25 §:n mukaisesti Säteilyturvakeskuksen on liitettävä periaatepäätöshakemuksesta antamaansa alustavaan turvallisuusarvioon YEL 56 § 2 momentissa tarkoitetun neuvottelukunnan lausunto. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

6.2 Rakentamislupavaihe

602. Rakentamislupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja YEA 35 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuusarviota valmistellessaan STUK pyytää sisäministeriöltä lausunnon YEA 35 §:n 1 momentin kohdassa 6 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15]. **[**Selkeytys ja pieni muutos, korjattu sisäasiainministeriö sisäministeriöksi **]**

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. Edellä mainituille suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.2 on mainittu. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

604. Rakentamislupahakemuksen käsittelyn aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

605. Rakentamislupahakemuksen käsittelyn aikana STUK voi osallistua harkintansa mukaan tietoturvatarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**Selkeytys ja pieni muutos, lisätty kenelle ilmoitettava **]**

6.3 Rakentamisvaihe

606. Luvussa 5.3 mainituille suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.3 on mainittu. STUK todentaa edellä mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

607. Rakentamisen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

608. STUK voi osallistua harkintansa mukaan rakentamisen aikaisiin tietoturvatarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

6.4 Käyttölupavaihe

609. Käyttölupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja YEA 36 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuuden kokonaisarviota valmistellessaan STUK käsittelee myös tietoturvallisuuden hallintaa ja pyytää sisäministeriöltä lausunnon YEA 36 §:n 1 momentin kohdassa 7 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15]. **[**Selkeytys ja pieni muutos, sisäasiainministeriö - sisäministeriö **]**

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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

611. Käyttölupavaiheen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

6.5 Käyttövaihe

612. Suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.5 on mainittu. 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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

613. Käytön aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**Selkeytys ja pieni muutos, kielellinen ulkoasu parannettu **]**

614. STUK voi osallistua harkintansa mukaan käytön aikaisiin tietoturvatarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**Selkeytys ja pieni muutos, Sana luvanhakija on poistettu. Kieliasua on parannettu. **]**

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. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

6.6 Käytöstäpoistovaihe

616. STUK valvoo käytöstäpoistovaiheessa suojattavien tietojen käsittelyä harkintansa mukaan. **[**Selkeytys ja pieni muutos, selkeytetty kuvauksen tekstiä **]**

617. POISTETTU. STUK valvoo, että tietoturvakontrollit ovat riittävät uhkien ja lainvastaisen sekä luvattoman toiminnan torjumiseen ja ydinturvallisuuden varmistamiseen myös käytöstäpoistovaiheessa. **[**Selkeytys ja pieni muutos, Poistettu, kattavammin muotoiltu: "uhkien ja lainvastaisen sekä luvattoman toiminnan torjumiseksi", käsittää siis myös muut kuin lainvastaisen ja luvattoman toiminnan aiheuttamat uhat. Poistettu L1 jälkeen, koska päällekkäinen edellisen kohdan kanssa. **]**

618. POISTETTU. STUK todentaa käytöstäpoistovaiheeseen liittyvien asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**Poistettu, Poistettu, koska päällekkäinen 616 kanssa. **]**

7 Viitteet

1. Ydinenergialaki (990/1987). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

2. Säteilyturvakeskuksen määräys ydinenergian käytön turvajärjestelyistä (STUK Y/3/2016). **[**Muutos säädösviittaukseen, VNA korvattu määräyksellä STUK Y/3/2016 **]**

3. Säteilyturvakeskuksen määräys ydinvoimalaitoksen turvallisuudesta (STUK Y/1/2018). **[**Muutos säädösviittaukseen, VNA korvattu Määräyksellä STUK Y/1/2018 **]**

4. Laki viranomaisten toiminnan julkisuudesta (621/1999). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

5. POISTETTU. ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security management. **[**Poistettu, Korvattu viitteellä ISO/IEC 27000 -standardisarjaan. **]**

6. POISTETTU. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden Hallintajärjestelmät. Vaatimukset. **[**Poistettu, Viite 19 korvaa yksittäiset luvut. **]**

7. POISTETTU. ISO/IEC 27005. Information technology – Security techniques – Information security risk management. **[**Poistettu, Korvattu viitteellä koko ISO/IEC 27000 -standardisarjaan. **]**

8. POISTETTU. IEC 62443 -sarja. **[**Poistettu, Siirretään perustelumuistioon. **]**

9. POISTETTU.Vahti 6/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. **[**Poistettu, Korvattu perustelumuistion viitteellä VAHTI-ohjeistukseen. **]**

10. POISTETTU. Vahti 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. **[**Poistettu, Korvattu perustelumuistion viitteellä VAHTI-ohjeistukseen. **]**

11. POISTETTU. Vahti 1/2013. Sovelluskehityksen tietoturvaohje. **[**Poistettu, Korvattu perustelumuistion viitteellä VAHTI-ohjeistukseen. **]**

12. POISTETTU. COBIT. Control Objectives for Information and Related Technology. **[**Poistettu, COBIT esittelee hyviä käytäntöjä, mutta siinä on paljon muutakin kuin tietoturvaa. **]**

13. KATAKRI II kansallinen turvallisuusauditointikriteeristö, kuitenkin uusin EK:n vahvistama versio. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

14. POISTETTU. NIST 800 -sarja. **[**Poistettu, NIST 800 -sarja on tarkoitettu tukemaan tiettyjen Yhdysvaltalaisten vaatimusten täyttymistä, sitä ei voi edellyttää Suomessa. **]**

15. Ydinenergia-asetus (161/1988). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

16. Valtioneuvoston asetus ydinenergia-asetuksen muuttamisesta (755/2013). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

17. POISTETTU. Säteilyturvakeskuksen määräys ydinjätteiden loppusijoituksen turvallisuudesta (STUK Y/4/2018). **[**Poistettu, Viitettä ei ole käytetty vaatimuksissa. **]**

18. POISTETTU. ISO/IEC 31000. Riskienhallinta. Periaatteet ja ohjeet. **[**Poistettu, ISO/IEC 31000 koskee yleistä riskienhallintaa, joten se on korvattu viitteellä ISO/IEC 27000 -standardisarjaan. **]**

19. SFS-EN ISO/IEC 27000:2017 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

20. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

21. Neuvoston päätös, annettu 23 päivänä syyskuuta 2013, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

22. VAHTI-ohjeistus, www.vahtiohje.fi. **[**[Muutoksen tyyppi], [Muutoksen perustelut] **]**

Määritelmät

Järjestelmä (tietoturvallisuuteen liittyvä) (system (information security))
Tietoturvallisuuteen liittyvällä järjestelmällä tarkoitetaan ihmisistä, 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. **[**Selkeytys ja pieni muutos, sanaan ihmisistä korjattu pieni i **]**

Riskianalyysi (risk analysis)
Riskianalyysillä tarkoitetaan järjestelmällisin menetelmin tehtäviä selvityksiä uhkien, ongelmien ja haavoittuvuuksien tunnistamiseksi, niiden syiden ja seurauksien kartoittamiseksi sekä niihin liittyvien riskien arvioimiseksi. (STUK Y/3/2016) **[**Muutos säädösviittaukseen, VNA => STUKin määräys **]**

Tietoturvallisuuden hallintajärjestelmä (information security management system)
Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan sitä osaa ydinlaitoksen yleisestä johtamisjärjestelmästä, joka luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan jatkuvasti. Tietoturvallisuuden hallintajärjestelmä sisältää organisaatiorakenteen, tietoturvallisuuden hallintapolitiikan, suunnittelutoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit ja resurssit. **[**Selkeytys ja pieni muutos, kirjoitusvirhe korjattu, "johtamisjärjestelmästä" yksi ä poistettu **]**

Turvajärjestelyt (security arrangements)
Turvajärjestelyillä tarkoitetaan ydinenergian käytön turvaamiseksi lainvastaiselta toiminnalta tarvittavia toimenpiteitä ydinlaitoksessa, sen alueella, muussa paikassa tai kulkuvälineessä, jossa ydinenergian käyttöä harjoitetaan. (YEL 990/1987) **[**Selkeytys ja pieni muutos, Teksti muutettu YEL:n mukaiseksi, "taikka"-sana poistettu **]**