OHJE YVL A.12

YDINLAITOKSEN TIETOTURVALLISUUDEN HALLINTA

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.20yy 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/3/2018) säädettyjä suunnitteluvaatimuksia. Määräyksen 4 §:n mukaan ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa on käytettävä kehittyneitä tietoturvallisuusperiaatteita. Luvaton pääsy ydinlaitoksen suojaus-, ohjaus- ja säätöjärjestelmiin on estettävä. **[**Muutos säädösviittaukseen, VNA 734/2008 korvattu STUK Y/3/2018 **]**

102. Turvajärjestelyjä, mukaan lukien tietoturvallisuus, koskevien asiakirjojen julkisuudesta on voimassa se, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) [4] säädetään. Vaitiolovelvollisuudesta säädetään ydinenergialain (990/1987) 78 §:ssä [1]. Vaitiolovelvollisuus koskee myös turvajärjestelyjä koskevia suunnitelmia. **[**Selkeytys ja pieni muutos, lisätty myös sana **]**

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

104. Tietoturvallisuudella tarkoitetaan tietojen, tietoturvallisuuteen liittyvien järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen eheyttä, kiistämättömyyttä, käytettävyyttä ja luottamuksellisuutta turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. Tietoturvallisuus on osa luvanhaltijan johtamisjärjestelmää ja turvajärjestelyjä. **[**N/A, N/A **]**

105. Tietoturvallisuus kattaa tiedon eheyden, kiistämättömyyden, käytettävyyden ja luottamuksellisuuden turvaamisen sen kaikissa olomuodoissaan aina tiedon luomisesta sen tuhoamiseen asti. Tiedolla tarkoitetaan eri muodossa talletettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisenä paperiasiakirjana, tiedostona, tietokantana tai suoritettavana ohjelmana, filmillä tai ääni- tai kuvatallenteena. **[**N/A, N/A **]**

2 Soveltamisala

201. Tässä ohjeessa esitetään ydinlaitosten 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 sekä muuhun ydinenergian käyttöön. 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

[Selkeytys ja pieni muutos, Tietoturvallisuuden kannalta tärkeitä vaatimuksia kuvataan luettelossa mainituissa ohjeissa. **]**

3 Tietoturvallisuuden hallinta

3.1 Tietoturvallisuuden hallintajärjestelmä

301. Ydinlaitoksen johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintaan. **[**N/A, N/A **]**

302. Luvanhakijalla ja luvanhaltijalla on oltava tietoturvallisuuden hallintajärjestelmä, joka on osa johtamisjärjestelmää. **[**Selkeytys ja pieni muutos, Jaettu, lisätty luvanhakija ja muokattu tekstiä,jaettu **]**

302a. Tietoturvallisuuden hallintajärjestelmän on täytettävä ohjeen YVL A.3 "Turvallisuuden johtaminen ydinalalla" vaatimukset. **[**Jaettu, 302 tietoturvallisuuden hallintajärjestelmä ja 302a johtamisjärjestelmä sen on täytettävä A.3 vaatimukset **]**

303. Tietoturvallisuuden hallintajärjestelmän on katettava hallinnolliseen tietoturvallisuuteen liittyvät toimenpiteet ja menettelyt. **[**Selkeytys ja pieni muutos, Jaettu, 303 hallinnolliseen tietoturvaan liittyvät toimenpiteet ja menettelyt 303a tekniseen tietoturvaan liittyvät toimenpiteet ja menettelyt 303b ulkoisten resurssien ohjaaminen ja valvonta tietoturvallisuuden osalta **]**

303a. Tietoturvallisuuden hallintajärjestelmän on katettava tekniseen tietoturvallisuuteen liittyvät toimenpiteet ja menettelyt. **[**Jaettu, hallinnollinen tietoturva 303 tekninen tietoturva 303a **]**

303b. Tietoturvallisuuden hallintajärjestelmän tulee sisältää myös 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, jaettu kansaiväliset ja kansallliset ohjeistukset 304 kansainväliset **]**

304a. Kansalliset ohjeistukset [9–11, 13] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin. **[**Jaettu, jaettu kansaiväliset ja kansallliset ohjeistukset **]**

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 luvanhaltijan ja luvanhakijan on ylläpidettävä hyvää turvallisuuskulttuuria. Tietoturvallisuudesta huolehtiminen on osa hyvää turvallisuuskulttuuria. **[**Muutos

säädösviittaukseen, VNA korvatty STUK Y määräyksellä, 2018 L4-versiosta tarkastettu **]**

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. **[**N/A, N/A **]**

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

309. Tietoturvallisuuden tavoitteet on esitettävä osana tietoturvallisuuden hallintajärjestelmää. **[**Jaettu, useita vaatimuksia yhden vaatimuksen alla, jaettu omikseen **]**

309a. Tietoturvallisuustavoitteiden saavuttamista on seurattava ja tavoitteita on arvioitava jatkuvan parantamisen periaatetta noudattaen. **[**Selkeytys ja pieni muutos, Jaettu, useita vaatimuksia yhden vaatimuksen alla, jaettu omikseen **]**

309b. Toteutussuunnitelmissa on esitettävä toimijoiden vastuut ja velvollisuudet, toimenpiteet, resurssitarpeet, toteutus- ja ylläpitoaikataulut sekä se, kuinka toimenpiteiden vaikuttavuutta arvioidaan ja kehitetään. **[**Jaettu, useita vaatimuksia yhden vaatimuksen alla, jaettu omikseen **]**

310. Tietoturvallisuusorganisaatio on kuvattava tietoturvallisuuden hallintajärjestelmässä. Kuvauksessa on otettava huomioon myös ulkoiset toimijat ja näiden vastuut. **[**Jaettu, Selkeytys ja pieni muutos, useita vaatimuksia yhden vaatimuksen alla, jaettu omikseen, tekstiä muokattu **]**

310a. Tehtävät ja vastuualueet on tarpeen mukaan eriytettävä, jotta vähennetään organisaation suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. **[**Jaettu, selkeytys, vaatimus 310 jaettu 310a ja tekstiä muokattu **]**

311. Luvanhaltijan on dokumentoitava, mitä kriteereitä ja standardeja hyödyntäen tietoturvallisuuden hallintajärjestelmä on toteutettu. **[**Selkeytys ja pieni muutos, Jaettu, 311 vaatimuksessa useampi vaatimus, jaettu **]**

311a. Viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen on käytettävä viranomaisen noudattamia menettelyjä [10] ja suojauksen tietoturvallisuuden arviointiin voidaan käyttää KATAKRI-kriteeristöä [13]. **[**Jaettu, Selkeytys ja pieni muutos, 311 vaatimuksessa useampi vaatimus, jaettu **]**

311b. Ennen viranomaisen turvallisuusluokittelemaa, salassa pidettävää tai näistä johdettua tietoa sisältävän aineiston luovuttamista kolmannelle osapuolelle. Luvanhaltijan tai luvanhakijan on haettava aineiston laatineen viranomaisen hyväksyntä tiedon luovuttamiselle. **[**Jaettu, Selkeytys ja pieni muutos, aikaisempaa vaatimusta laajennettu huomioimaan paremmin viranomaisasiakirjan käsittelyä JulkL **]**

312. Tietoturvallisuusriskien arvioinin ja hallinnan menettelyjen on oltava osa tietoturvallisuuden hallintajärjestelmää, riskejä on arvioitava kuhunkin aihealueeseen ja järjestelmään parhaiten soveltuvilla menetelmillä. **[**Jaettu, N/A **]**

312a. Luvanhaltijan on varmistettava, että tietoturvallisuusriskien arviointiin käytetyt menettelyt ovat riittävät ja merkittävät riskit on tunnistettu. **[**Jaettu, N/A **]**

313. POISTETTU. Riskienhallinnan kokonaisuus on dokumentoitava. **[**Poistettu, Vanha vaatimus epäselvä, kirjoitettu uusiksi muualle **]**

314. POISTETTU. Luvanhaltijan on tehtävä tietoturvallisuuden uhka- ja riskienarviointi, ja se on päivitettävä vuosittain ja merkittävien tietoturvallisuutta koskevien tapahtumien, muutosten tai uusien uhkien ilmentyessä. **[**Poistettu, Päällekkäinen vaatimuksen 315 kanssa **]**

315. Tietoturvallisuuteen liittyvät uhkat ja riskit on systemaattisesti analysoitava, ja suojaavat toimenpiteet ja menetelmät valittava analyysin perusteella. Analyysiä on ylläpidettävä ja kehitettävä. **[**N/A, N/A **]**

316. Suojattavat kohteet on tunnistettava ja määriteltävä riittävän yksityiskohtaisesti. **[**Jaettu, Selkeytys ja pieni muutos, sanamuotoa muokattu, 316 oli useampi vaatimus, jaettu **]**

316a. Suojattaviin kohteisiin liittyvät uhkat ja haavoittuvuudet sekä tietoturvallisuusloukkausten aiheuttamat vaikutukset on arvioitava ja niiden perusteella on määriteltävä tarpeelliset suojaustoimenpiteet. **[**Jaettu, 316 oli useampi vaatimus, jaettu **]**

316b. Suojaustoimenpiteet on dokumentoitava. **[**Jaettu, 316 oli useampi vaatimus, jaettu **]**

317. Pääsyä suojattaviin kohteisiin on valvottava lokimenettelyin, lokimerkintöjen tulee sisältää riittävät tiedot tapahtuman ja käyttäjän jäljittämiseen. **[**Jaettu, 317 oli useampi vaatimus, jaettu **]**

317a. Lokitiedostot on suojattava asiattomilta muutoksilta. **[**Jaettu, 317 oli useampi vaatimus, jaettu **]**

3.2 Asiakirjoja koskevat vaatimukset

318. Luvanhaltijan asiakirjoja koskevat yleiset vaatimukset on esitetty ohjeissa YVL A.1 "Ydinenergiankäytön turvallisuusvalvonta", YVL A.3 "Turvallisuuden johtaminen ydinalalla" ja YVL A.11 "Ydinlaitoksen turvajärjestelyt", ja näitä on noudatettava tietoturvallisuutta koskevissa asiakirjoissa. **[**Selkeytys ja pieni muutos, lisätty ohjeiden nimet **]**

319. Asiakirjat on luokiteltava niiden tietoturvallisuus- ja turvallisuusmerkityksen mukaan. **[**Jaettu, Selkeytys ja pieni muutos, useampi vaatimus sisällytetty yhteen vaatimukseen. Nyt jaettu ja tekstiä muokattu sopivammaksi. **]**

319a. Asiakirjoja on suojattava luokituksen mukaisesti luvattomalta käytöltä, muuttamiselta ja tuhoamiselta. Asiakirjojen saatavuus luvalliselle käyttäjälle on turvattava. **[**Jaettu, Selkeytys ja pieni muutos, useampi vaatimus sisällytetty yhteen vaatimukseen. Vaatimus jaettu kahteen osaan ja tekstiä selkeytetty. **]**

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 teknologiset resurssit. **[**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, asiakirjojen suojaus ja luokitus tässä omana vaatimuksen kohtana **]**

321. Keskeisten tietoturvallisuuden hallintaan liittyvien henkilöiden ja muiden resurssien on oltava luvanhakijan/luvanhaltijan palveluksessa tai omistuksessa. **[**Jaettu, vaatimus jaettu kahteen. 321 riittävät resurssit käyttettävissä. 321a ulkoistamista koskeva riskiarvio **]**

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 jaettu kahteen. 321 riittävät resurssit käyttettävissä. 321a ulkoistamista koskeva riskiarvio **]**

322. Tietoturvallisuuden kouluttamiseen, kehittämiseen ja ylläpitoon osallistuvien henkilöiden koulutus ja osaamisen ylläpito on oltava riittävää heidän tietoturvallisuuteen liittyvien tehtäviensä toteuttamiseksi. **[**Jaettu, useampi vaatimus samassa, jaetu 322 tietoturvallisuuden

osaaminen ja koulutus 322a resurssien osaaminen ja koulutus **]**

322a. Ydinlaitoksen koko henkilökunnan sekä ulkoisten resurssien on oltava tietoisia tietoturvallisuuden hallintaan liittyvistä asioista tehtäviensä asianmukaisen hoitamisen kannalta riittävässä määrin. **[**Jaettu, useampi vaatimus samassa, jaetu 322 tietoturvallisuuden osaaminen ja koulutus 322a resurssien osaaminen ja koulutus 322b koulutustaphtumien dokumentointi **]**

322b. Tietoturvallisuuteen liittyvät koulutustapahtumat on dokumentoitava. **[**Jaettu, useampi vaatimus samassa, jaetu 322 tietoturvallisuuden osaaminen ja koulutus 322a resurssien osaaminen ja koulutus 322b koulutustaphtumien dokumentointi **]**

323. Ulkoisten resurssien käytön osalta luvanhaltijan on sopimuksin ja tarkastusmenettelyiden avulla huolehdittava, että niiden tietoturvallisuuden taso ja vastuujärjestelyt ovat vähintään samalla tasolla kuin luvanhaltijalla vastaavissa toimissa. **[**Jaettu, Selkeytys ja pieni muutos, vaatimus 323 jaettu useamman vaatimuksen takia, 328:sta siirretty viitaus ohjeiden YVL A3. ja A.5 vaatimukset toimittajien valvonnalle 323a.:han **]**

323a. Luvanhaltijan on esitettävä ne toimenpiteet, joilla se valvoo toimittajaosapuolen tai muun vastaavan ulkoisen resurssin tietoturvallisuutta. Varmistuksissa on huomioitava mahdolliset 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 jaettu useamman vaatimuksen takia, 328:sta siirretty viitaus ohjeiden YVL A3. ja A.5 vaatimukset toimittajien valvonnalle 323a.:han **]**

3.4 Tietoturvallisuuden hallintajärjestelmän tarkastukset ja katselmoinnit

324. Tietoturvallisuuden riittävyyden todentamiseksi luvanhaltijan on järjestettävä tietoturvallisuuden itsearviointi vuosittain siten, että tietoturvallisuuden hallintajärjestelmän kaikki osa-alueet arvioidaan vähintään kolmen vuoden välein. Arvioinnin yhteydessä on selvitettävä myös mahdolliset riskienarviointiin ja uhkakuvaan tulleet muutokset sekä ajanjaksolla ilmenneiden tietoturvallisuustapahtumien merkitys hallintajärjestelmälle. **[**N/A, N/A **]**

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, poistettu väli asiantujaryhmän välistä. **]**

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. **[**N/A, N/A **]**

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. **[**N/A, N/A **]**

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, asia käsitellään vaatimuksessa 323a.:ssa **]**

329. Tarkastukset, arvioinnit ja katselmoinnit on dokumentoitava. **[**Selkeytys ja pieni muutos, lisätty vielä arvioinnit, mahdollisesti vaatii täytäntöönpanon **]**

3.5 Tietoturvallisuuden hallintajärjestelmän parantaminen

330. Jatkuvassa parantamisessa on hyödynnettävä sekä oman että muiden toimialojen tietoturvallisuuden hallinnasta saatuja käyttökokemuksia. **[**N/A, N/A **]**

331. Luvanhaltijan johdon on edistettävä tapoja, joilla koko henkilökunta osallistuu tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja jatkuvaan parantamiseen. **[**N/A, N/A **]**

332. Luvanhaltijan johdon on varmistettava, että tietoturvallisuuden hallintajärjestelmään kohdistuvat parannukset ovat asetettujen tavoitteiden mukaisia. **[**Selkeytys ja pieni muutos, lisätty viittaus tietoturvallisuuteen -"tietoturvallisuuden hallintajärjestelmään" **]**

4 Turvallisuuden kannalta tärkeiden järjestelmien suojaaminen

401. Säteilyturvakeskuksen määräyksen STUK Y/3/2018 4 §:n mukaisesti ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa ja ylläpidossa on käytettävä kehittyneitä, tarkoituksenmukaisia tietoturvallisuusperiaatteita. **[**Muutos säädösviittaukseen, Selkeytys ja pieni muutos, Valtioneuvoston asetus (734/2008) korvattu STUK Y/3/2018, maininta luvattomasta pääsystä siirretty 402. **]**

4.1 Yleiset vaatimukset

402. Ydinlaitoksen turvallisuuteen vaikuttavien laitteiden ja järjestelmien, kuten tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmien, tietoturvallisuus ja arkkitehtuuri on suunniteltava ja toteutettava siten, että luvaton pääsy on estetty riittävien fyysisten, teknisten ja hallinnollisten turvajärjestelyjen avulla niin hyvin kuin käytännöllisin toimenpitein on mahdollista. **[**Selkeytys ja pieni muutos, Selkeytettiin tekstiä ja lisättiin "laitteet" STUK in määräyksen mukaiseksi. **]**

403. Asiaankuulumattomien laitteiden asentaminen on estettävä luotettavasti koko elinkaaren ajan. **[**Jaettu, Selkeytys ja pieni muutos, vaatimuksessa kaksi asiaa, toinen jaettu 403a, 403b lisätty E.7 siirretty käynnit sähkö ja automaatiojärjestelmien. Huomioitu laitoksen koko elinkaari **]**

403a. Asiaankuulumattomien ohjelmien asentaminen on estettävä luotettavasti koko elinkaaren ajan. **[**Jaettu, Selkeytys ja pieni muutos, useampi vaatimus samassa, jaettu, Huomioitu laitoksen koko elinkaari **]**

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

404. Ydinlaitoksen laitteet ja järjestelmät sekä turvavalvonnan järjestelmät ja valmiustoiminnan viestintäjärjestelmät on suojattava tietoturvallisuuteen liittyvien vyöhykkeiden ja ohjeen YVL A.11 vaatimien turvajärjestelyvyöhykkeiden tason mukaisesti. **[**Selkeytys ja pieni muutos, selkeytetty kielellisesti **]**

405. Verkottuneet laitteet kattavat kaikki ne laitteet, jotka on liitetty toiseen laitteeseen tietoliikenteen mahdollistavalla verkolla/kaapelilla. Näihin liittyvät kaapeloinnit ja tietoliikenne on suojattava lainvastaiselta tai luvattomalta toiminnalta. **[**Jaettu, N/A **]**

405a. Verkkojen fyysinen ja looginen erottelu on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen. **[**Jaettu, N/A **]**

405b. Verkkojen tietoliikenteen valvonta on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen.
[Jaettu, N/A **]**

405c. (E.7 635.) Ydinlaitoksen turvallisuuden kannalta keskeisiin ohjelmistopohjaisiin järjestelmiin ei saa olla fyysistä mahdollisuutta muodostaa tiedonsiirtoyhteyttä järjestelmän

ulkopuolelta sisäänpäin. **[**Siirretty, Vaatimus on siirretty ohjeesta YVL E.7. **]**

405d. (B.1 5244.) Automaation suojausjärjestelmä on erotettava toiminnallisesti muista automaatiojärjestelmistä siten, että verkotettu tiedonsiirto on estetty suojausjärjestelmään 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. **]**

406. Luvanhaltijan on rajoitettava yksittäisen henkilön mahdollisuutta asentaa haitallinen toiminnallisuus useisiin rinnakkaisiin samaa suojaustehtävää suorittaviin laitteisiin tai järjestelmiin. **[**Jaettu, Selkeytys ja pieni muutos, tekstiä selkeytetty, 406 jaettu kolmeen osaan, koska sisälsi usemman vaatimuksen **]**

406a. Yksittäisen ohjelmiston haitallinen vaikutus ydinlaitoksen turvallisuuteen on tehtävä niin pieneksi kuin käytännöllisin keinoin on mahdollista. **[**Jaettu, 406 jaettu kolmeen osaan, koska sisälsi usemman vaatimuksen **]**

406b. Haitallisen toiminnallisuuden asentaminen tai suojaustoiminnon lamauttaminen on voitava havaita luotettavasti. **[**Jaettu, tekstiä selkeytetty, 406 jaettu kolmeen osaan, koska sisälsi usemman vaatimuksen **]**

407. POISTETTU. Ydinlaitoksen ja sen tieto-, tietoliikenne-, automaatio-, sähkö-, turvavalvonta- ja viestintäjärjestelmiä koskevat asiakirjat ja tiedot on niiden turvallisuusmerkityksen mukaisesti suojattava siten, että vain henkilöt, joilla on oikeus niiden käsittelyyn voivat saada ne haltuunsa. **[**Poistettu, Päällekkäinen luvun 3.3 vaatimusten kanssa. **]**

4.2 Tietoliikenteen ja ICT-palveluiden hallinta ja kontrollointi

408. Luvanhaltijalla on oltava kirjalliset menettelyohjeet turvallisille tietojenkäsittelypalveluille. **[**Jaettu, kaksi vaatimusta 408 sisällä, jaettu kahteen **]**

408a. Ohjeita on ylläpidettävä ja niiden on oltava kaikkien niitä tarvitsevien käyttäjien saatavilla. **[**Jaettu, kaksi vaatimusta 408 sisällä, jaettu kahteen **]**

409. Konfiguraatiohallinnassa on huomioitava tietoturvallisuus. **[**Selkeytys ja pieni muutos, selkeytys, kuvaa paremmin mitä halutaan. **]**

4.3 Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito

410. Tietoturvallisuudesta tulee huolehtia tietoturvallisuuteen liittyvien järjestelmien kaikissa elinkaaren vaiheissa. Luvanhaltijan on kiinnitettävä myös huomiota ennakoivaan tietoturvallisuuteen sekä käyttökokemusten keräämiseen ja hyödyntämiseen. **[**Selkeytys ja pieni muutos, tekstiä selkeytetty **]**

411. POISTETTU. Järjestelmien hankintaan, kehitykseen ja ylläpitoon liittyvän tietoturvallisuusdokumentaation on oltava kattavaa ja ajantasaista. Dokumentaation on selkeästi liityttävä muuhun järjestelmädokumentaatioon. **[**Poistettu, Kuuluu osaksi järjestelmädokumentaatiota **]**

412. POISTETTU. Järjestelmien ja niiden osakomponenttien väliset toiminnalliset riippuvuudet on tunnistettava ja niiden vaikutus tietoturvallisuuteen on analysoitava ja arvioitava sekä poistettava haitalliset riippuvuudet. **[**Poistettu, e.7 vastaa jo automaation osalta vaatimuksista. **]**

413. Verkottuneiden järjestelmien osalta on kuvattava kattavasti ja yksiselitteisesti eri järjestelmien rajapinnat, yhteydet, käytetyt protokollat sekä kommunikoivat osapuolet. **[**N/A, N/A **]**

414. Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä. **[**N/A, N/A **]**

4.4 Tietoturvallisuuspoikkeamien hallinta

415. Tietoturvallisuuden hallintajärjestelmässä on oltava menettelyt tietoturvallisuuspoikkeamien tunnistamiseen, selvittämiseen ja käsittelyyn. Poikkeamien hallinnan vaatimukset on kuvattu ohjeessa YVL A.3. **[**Selkeytys ja pieni muutos, selkeytetty, viittaus ohjeeseen A.3 **]**

416. POISTETTU. Luvanhaltijan on luotava menettelyt järjestelmälliseen reagointiin tietoturvallisuuspoikkeamien varalta. **[**Poistettu, PÄÄLLEKKÄINEN 415 KANSSA **]**

417. Tietoturvallisuuspoikkeamien ilmoittamiseen on luotava menettelyt. STUKille on ilmoitettava kaikki ydinturvallisuuden kannalta merkittävät tietoturvallisuuspoikkeamat viipymättä. **[**Selkeytys ja pieni muutos, poistettu lause poikkeamien hallintaan liittyen ohjeeseen YVL A.3 joka on huomioitava. **]**

4.5 Käyttöoikeuksien hallinta

418. Käyttöoikeuksien hallintaperiaatteet on laadittava, dokumentoitava ja katselmoitava. **[**Selkeytys ja pieni muutos, korvattu valvontaperiaatteet hallintaperiaatteilla **]**

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

418b. (421.) Salasanapolitiikka on määriteltävä ja otettava käytäntöön. **[**Siirretty, Selkeytys ja pieni muutos, Vaatimus 421 siirretty. Poistettu teksti: "Toteutumista on valvottava." **]**

419. Eri järjestelmien pääkäyttäjäoikeudet on rajoitettava. Käyttöoikeudet on myönnettävä vain työtehtävien mukaisesti. **[**N/A, N/A **]**

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

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

422. Etätyöhön ja ulkoisten resurssien tekemään työhön on luotava turvallisen tietojenkäsittelyn menettelyt ja näiden noudattamista on valvottava. **[**Selkeytys ja pieni muutos, järjestelmien käyttö jätetty tästä pois **]**

4.6 Turvallisuuteen liittyvien järjestelmien tietoturvallisuustestaaminen

423. Turvajärjestelyjen valvontaan liittyvien järjestelmien tietoturva on testattava. Tietoturvan testaamista 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. **]**

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

425. Tietoturvallisuuden kannalta tärkeiden verkottuneiden järjestelmien testaamisessa on käytettävä kehittyneitä testaamismenettelyjä. **[**Selkeytys ja pieni muutos, selkeytetty tekstiä ja poistettu päällekäisyyttä **]**

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]. **[**N/A, N/A **]**

5.2 Rakentamislupavaihe

502. Rakentamislupahakemuksen yhteydessä luvanhakijan on toimitettava seuraavat asiakirjat STUKille hyväksyttäväksi:

1. Luvanhakijan tietoturvallisuuden hallintapolitiikka ja tietoturvallisuuden hallintajärjestelmän kuvaus, josta saadaan kokonaisvaltainen käsitys tietoturvallisuudesta.
2. Tietoturvallisuuden arviointisuunnitelma sekä analyysi tietoturvallisuuteen liittyvistä uhkista ja riskeistä.

3. Laitostason tietoturvallisuusvaatimukset.
4. Tietoturvallisuuden arkkitehtuurisuunnitelma, mukaan lukien kuvaus järjestelmien välisistä yhteyksistä.
5. Kuvaus luvanhakijan tietoturvallisuusorganisaatiosta rakentamisvaihetta varten.
6. Suunnitelma ydinlaitoksen rakentamisen aikaisista toimittajiin kohdistuvista tietoturvallisuuden valvontatoimista.
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. **[**Selkeytys ja pieni muutos, muokkauksia /tarkennuksia vaadittuihin asiakirjoihin, lisätty säädösviittaus YEA 1988/161 35§ **]**

503. Seuraava asiakirja on toimitettava STUKille tiedoksi:
Asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittyvät kuvaukset. **[**Selkeytys ja pieni muutos, listaus asiakirjoista poistettu, vaatimus 502 sisältää rakennuslupahakemuksen yhteydessä toimitettavat asiakirjat **]**

504. Perustelluista syistä vaatimuksessa 503 esitetty asiakirja voidaan STUKille toimittamisen sijasta todentaa myös rakentamisluvan hakijan osoittamassa paikassa. **[**Selkeytys ja pieni muutos, korvattu kohdassa sanalla vaatimuksessa **]**

505. POISTETTU. Vaatimuksissa 502 ja 503 esitetyt asiakirjat on pidettävä ajan tasalla. **[**Poistettu, esitetty asia on kappaleessa 5.3 KAPPALE **]**

5.3 Rakentamisvaihe

506. Ydinlaitoksen rakentamisen aikana STUKin hyväksyttäväksi on toimitettava seuraavat asiakirjat:
1. Vaatimuksen 502 asiakirjojen merkittävät muutokset.
2. Rakentamisvaiheen tietoturvallisuuden arviointisuunnitelma sekä analyysi tietoturvallisuuteen liittyvistä uhkista ja riskeistä.
3. Järjestelmäkohtaiset tietoturvasuunnitelmat.
4. Järjestelmäkohtaiset tietoturvallisuuden testaussuunnitelmat. **[**Selkeytys ja pieni muutos, muokattu luetteloa:3. Järjestelmäkohtaiset tietoturvasuunnitelmat. ja 4. Järjestelmäkohtaiset tietoturvallisuuden testaussuunnitelmat **]**

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

2. tietoturvallisuuden katselmointiraportit
3. tietoturvallisuuden testausraportit
4. päivitetyt tietoturvallisuussuunnitelmat. **[**Selkeytys ja pieni muutos, muokattua toimitettavien asiakirjojen luetteloa **]**

508. Perustelluista syistä vaatimuksessa 507 esitetyt asiakirjat voidaan STUKille toimittamisen sijasta todentaa myös rakentamisluvan hakijan osoittamassa paikassa. **[**N/A, N/A **]**

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, asiakirjojen päivityksestä vaatimus 506, 507 **]**

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. Tietoturvallisuuden hallintajärjestelmän kuvaus.
2. Tietoturvallisuusriskien arviointisuunnitelma ja käytön aikaisten riskien arviointia koskevat tulokset.
3. Järjestelmätasoiset tietoturvallisuuskuvaukset, tietoturvallisuuteen liittyvien vyöhykkeiden kuvaus ja kokonaisarkkitehtuurikuvaus.
4. Kuvaus luvanhakijan käyttövaiheen tietoturvallisuusorganisaatiosta. **[**Selkeytys ja pieni muutos, muokattu tekstiä, listattu käyttölupahakemuksen käsittelyä varten tarvittavat asiakirjat **]**

5.5 Käyttövaihe

512. Käyttövaiheessa luvanhakijan on toimitettava seuraavat asiakirjat ja näiden päivitykset STUKille hyväksyttäväksi:

1. Tietoturvallisuuden hallintajärjestelmän kuvaus.
2. Tietoturvallisuusriskien arviointisuunnitelma ja käytön aikaisten riskien arviointia koskevat tulokset.
3. Järjestelmätasoiset tietoturvallisuuskuvaukset, tietoturvallisuuteen liittyvien vyöhykkeiden kuvaus ja kokonaisarkkitehtuurikuvaus.
4. Tietoturvallisuusvaatimukset ja kuvaus tietoturvallisuuden testaamismenettelyistä. **[**N/A, N/A **]**

513. Seuraavat asiakirjat ja näiden päivitykset on toimitettava STUKille tiedoksi:

1. Asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittyvät kuvaukset sekä tietosuojaus- ja menettelyohjeet.
2. Järjestelmien hankintaan ja ylläpitoon liittyvät tietoturvallisuusmenettelyohjeet.
3. Tietoturvallisuuden tavoitteet ja mittarit.
4. Tietoturvallisuuskoulutusohjelma.
5. Tietoturvallisuushäiriöihin liittyvät menettelyohjeet ja raportoinnit.
6. Tarkastusten ja katselmointien raportit.
7. Järjestelmien tietoturvallisuusdokumentaation ohjeistus (voi olla osana muuta dokumentaatiota) mukaan lukien tietoturvallisuustestaaminen ja näiden toteutuminen.
8. Järjestelmien suunnitteluohjeet mukaan lukien järjestelmien väliset yhteydet.
9. Kuvaus tunnistetuista suojattavista kohteista ja niihin liittyvistä suojausmenettelyistä.
10. Kuvaus tietoturvallisuusorganisaatiosta.
11. Ulkoisiin toimijoihin kohdistuvat tietoturvallisuuden valvontatoimet. **[**Selkeytys ja pieni muutos, korjattu liittävät sanaksi liitttyvät **]**

514. Perustelluista syistä tiedoksi toimitettavat asiakirjat tai vastaavat tiedot voidaan todentaa myös luvanhaltijan osoittamassa paikassa. **[**N/A, N/A **]**

5.6 Käytöstäpoistovaihe

515. Luvanhaltijan on toimitettava STUKille hyväksyttäväksi selvitys menettelyistä, joilla tietoturvallisuus toteutetaan käytöstäpoistovaiheen aikana ennen käytöstäpoistotoimien aloittamista. **[**N/A, N/A **]**

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. **[**N/A, N/A **]**

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. **[**N/A, N/A **]**

604. Rakentamislupahakemuksen käsittelyn aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**N/A, N/A **]**

605. Rakentamislupahakemuksen käsittelyn aikana STUK voi osallistua harkintansa mukaan luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin 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. **[**N/A, N/A **]**

607. Rakentamisen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**N/A, N/A **]**

608. STUK voi osallistua harkintansa mukaan rakentamisen aikaisiin luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**N/A, N/A **]**

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. **[**N/A, N/A **]**

611. Käyttölupavaiheen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**N/A, N/A **]**

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. **[**N/A, N/A **]**

613. Käytön aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset

voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa. **[**Selkeytys ja pieni muutos, kielellinen ulkoasu parannettu **]**

614. Käytön aikaisiin luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin ja katselmointeihin STUK voi osallistua harkintansa mukaan. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa. **[**Selkeytys ja pieni muutos, on ilmoitettava STUKille **]**

615. STUK valvoo tietoturvallisuuden hallintajärjestelmän toimintoja osana käytön valvonnan tarkastusohjelmaa. Lisäksi STUK tekee tarkastuksia luvanhaltijan pyynnöstä ja harkintansa mukaan. Tarkastukset voivat kohdistua luvanhaltijaan tai luvanhaltijan käyttämään toimittajaan. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. **[**N/A, N/A **]**

6.6 Käytöstäpoistovaihe

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

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

618. 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. **[**N/A, N/A **]**

7 Viitteet

1. Ydinenergialaki (990/1987). **[**N/A, N/A **]**

2. Säteilyturvakeskuksen määräys ydinenergian käytön turvajärjestelyistä (STUK Y/3/2018). **[**Muutos säädösviittaukseen, VNA korvattu määräyksellä STUK Y/3/2018 **]**

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

4. Laki viranomaisten toiminnan julkisuudesta (621/1999). **[**N/A, N/A **]**

5. ISO/IEC 27002. Information technology — Security techniques — Code of practice for

information security management. **[**N/A, N/A **]**

6. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden Hallintajärjestelmät. Vaatimukset. **[**N/A, N/A **]**

7. ISO/IEC 27005. Information technology – Security techniques – Information security risk management. **[**N/A, N/A **]**

8. IEC 62443 -sarja. **[**N/A, N/A **]**

9. Vahti 6/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. **[**N/A, N/A **]**

10. Vahti 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. **[**N/A, N/A **]**

11. Vahti 1/2013. Sovelluskehityksen tietoturvaohje. **[**N/A, N/A **]**

12. COBIT. Control Objectives for Information and Related Technology. **[**N/A, N/A **]**

13. KATAKRI II kansallinen turvallisuusauditointikriteeristö, kuitenkin uusin EK:n vahvistama versio. **[**N/A, N/A **]**

14. NIST 800 -sarja. **[**N/A, N/A **]**

15. Ydinenergia-asetus (161/1988). **[**N/A, N/A **]**

16. Valtioneuvoston asetus ydinenergia-asetuksen muuttamisesta (755/2013). **[**N/A, N/A **]**

17. Säteilyturvakeskuksen määräys ydinjätteiden loppusijoituksen turvallisuudesta (STUK Y/4/2018). **[**Muutos säädösviittaukseen, VNA => STUKin määräys **]**

18. ISO/IEC 31000. Riskienhallinta. Periaatteet ja ohjeet. **[**N/A, N/A **]**

19. IAEA, Computer Security at Nuclear Facilities, Series No. NSS17, 2011 **[**Uusi nimike, IAEA NSS17 nyt valmis, siihen viittaus **]**

20. Vahti 2/2014. Tietoturvallisuuden arviointiohje. **[**Uusi nimike, Vahti 2/2014 korvaa aikaisemmat Vahtiohjeet: Tietoturvallisuuden arviointi valtionhallinnossa VAHTI 8/2006 sekä Tietoturvallisuuden hallintajärjestelmänjärjestelmän arviointi suosituksen VAHTI 3/2003. **]**

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. **[**N/A, N/A **]**

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/3/2018) **[**Muutos säädösviittaukseen, VNA => STUKin määräys **]**

Tietoturvallisuuden hallintajärjestelmä (information security management system)
Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan sitä osaa ydinlaitoksen yleisestä johtamisjärjestelmästää, 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. **[**N/A, N/A **]**

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 **]**