

## TIETOTURVALLISUUDEN TARKASTUSLISTA (esim. suunniteltaessa ICT-hankintoja)

Tarkastuslista soveltuu pohjatyökaluksi ja sitä pitää soveltaa/kehittää oman toiminnan tarpeisiin.

|                                                                                                                                                                                                                                                                                                   |                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Yleiset tietoturvavaatimukset</b>                                                                                                                                                                                                                                                              |                                                               |
| Oletko huomionut:                                                                                                                                                                                                                                                                                 |                                                               |
| 1. että henkilötietoja tai muuta salassa pidettävää tietosisältöä ei saa välittää suojaamattomana Internetin yli (vaatimuksena on oltava esim. suojattu HTTPS-tiedonsiirto tai yritysVPN-tunneli)?                                                                                                | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 2. miten etäyhteyksien tietoturva toteutetaan ja yhteydenotot hallitaan (oletko selvittänyt mitkä vaihtoehdot ovat teknisesti mahdollisia kyseisessä järjestelmässä oman organisaatiosi ympäristössä)?                                                                                            | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 3. miten käytettävien palvelimien ja työasemien tietoturvallisuudesta (mm. virustorjunta ja muut päivitykset) huolehditaan? Huomioi/auditoi myös toimittajan tietoturvapolitiikka.                                                                                                                | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 4. että palvelun ja siihen liittyvän tietotekniikan riskienhallinnasta ja sen suunnittelusta huolehditaan ja kuka sen tekee? (Onko esim. tietojärjestelmiä varten varajärjestelmät sekä jatkuvuus- ja toipumissuunnitelmat ja puolueeton arvio hankittavan kokonaisuuden tietoturvasta olemassa?) | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 5. onko tietojen turvalliseen käsittelyyn, säilytykseen, varmuuskopiointiin ja hävittämiseen olemassa tarvittavat välineet ja toimintatavat (prosessit) ja onko niihin pyydetty kuvaus?                                                                                                           | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| <b>Käyttövaltuudet ja käytönvalvonta</b>                                                                                                                                                                                                                                                          |                                                               |
| Oletko huomionut:                                                                                                                                                                                                                                                                                 |                                                               |
| 6. miten hankittavassa järjestelmässä määritellään käyttöoikeudet (tukeeko se esim. roolipohjaisuutta) ja mitä salasanoihin liittyviä ehtoja voidaan asettaa (pituus, historia, muoto, vaihtoväli jne.)?                                                                                          | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 7. miten käyttäjät tunnistetaan ja mitä käyttäjätietoja tallennetaan?                                                                                                                                                                                                                             | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 8. miten järjestelmä on liitettävissä keskitettyyn käyttöoikeuksien hallintaan (IAM) ja/tai voidaanko järjestelmässä lukita ei-aktiiviset käyttäjätunnukset automaattisesti?                                                                                                                      | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 9. miten järjestelmä pystytään liittämään kertakirjautumiseen (SSO)?                                                                                                                                                                                                                              | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 10. että tarvittaessa pitää vaatia erilliset (kattavat ja tarkat) tietojen ja tietojärjestelmien käyttö- ja salassapitositoumukset?                                                                                                                                                               | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 11. että jälkikäteen pystytään yksilöidysti selvittämään, kuka on käsitellyt tietoja järjestelmästä, koska tämä on tapahtunut, miltä tietokoneelta ja mihin tietoihin toimenpide on kohdistunut?                                                                                                  | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 12. miten käytönvalvonta on toteutettu tai voidaan toteuttaa?                                                                                                                                                                                                                                     | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 13. oletko velvoittanut, että tietojärjestelmien käyttöoikeudet poistetaan tai niitä muutetaan, jos                                                                                                                                                                                               | <input type="checkbox"/> Kyllä                                |

|                                                                                                                                                                                                                                                                                                                              |                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| henkilö jää pois sopimuskumppanin palveluksesta tai hänen työtehtävänsä muuttuvat?                                                                                                                                                                                                                                           | <input type="checkbox"/> Ei                                   |
| 14. oletko varmistanut, että pääsy ohjelmointiympäristöön on rajoitettu ja sen käyttö on valvottu?                                                                                                                                                                                                                           | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| <b>Hankinnan kohde</b><br>Oletko huomionut                                                                                                                                                                                                                                                                                   |                                                               |
| 15. kuinka kriittinen järjestelmä on oman organisaation toiminnan kannalta? (Mikäli kriittinen, niin hankintaprosessiin pitää osallistua tietotekniikan ja juridiikan osaavia henkilöitä alusta lähtien.)                                                                                                                    | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 16. mikä on järjestelmän kriittisyysluokka poikkeusoloissa? Onko toimittajalle annettu selkeät ohjeet siitä, mitä tämä edellyttää?                                                                                                                                                                                           | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 17. soveltuuko järjestelmä oman organisaation tietoturva-arkkitehtuuriin, mukaan lukien eri määräykset ja ohjeet?                                                                                                                                                                                                            | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 18. ja tarkistanut toimittajalta, että onko järjestelmässä tietoturvaa heikentäviä ominaisuuksia ja onko se tarkastettu haittaohjelmien ja esim. testaukseen liittyneiden ns. takaporttien osalta?                                                                                                                           | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 19. tarkistaa, että onko järjestelmästä saatavissa sen tietoturva- ja tietosuojaoimaisuuksien dokumentaatio ja tarkistuslista?                                                                                                                                                                                               | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 20. tukeeko järjestelmä monikielisyyttä ja onko käyttöohjeet ja tuki saatavilla suomenkielellä?                                                                                                                                                                                                                              | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 21. ovatko järjestelmän tietoturvaominaisuudet kierrettävissä tai käyttäjien muutettavissa? (Jos ovat, niin voidaanko tämä mahdollisuus poistaa?)                                                                                                                                                                            | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 22. millaiset ovat järjestelmän rajapinnat muihin sovelluksiin päin? Tukeeko järjestelmä avoimia, yleisesti käytettyjä rajapintoja?                                                                                                                                                                                          | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 23. onko järjestelmä saatavissa koekäyttöön tai testaukseen?                                                                                                                                                                                                                                                                 | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 24. onko toimittaja aktiivisesti testannut ja kehittänyt tätä järjestelmää ja yleensä tuotteitaan?                                                                                                                                                                                                                           | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| <b>Sopimusasiat</b><br>Oletko huomionut                                                                                                                                                                                                                                                                                      |                                                               |
| 25. sopimuksessa, että oman organisaation tietosuojaan ja tietoturvaan liittyvät yhteyshenkilöt saavat viivyttämättä tiedon palveluun tai sen tietotekniikkaan liittyvistä tietoturva- ja tietosuojapoikkeamista/häiriöistä/ongelmista (esim. tietovuodot, hakkeroinnit, toteutuneet merkittävät riskit yms.)?               | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 26. onko sopimuksessa määritelty rahallinen sanktio mahdollisten tietovuotojen osalta?                                                                                                                                                                                                                                       | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 27. sopimusneuvotteluissa ja sopimuksissa, että edellytät toimittajan toimimaan voimassaolevan lainsäädännön ja oman organisaatiosi ohjeiden mukaisesti tietoturva- ja tietosuoja-asioissa eikä toimittaja saa luovuttaa mitään organisaatiosi omistamia tietosisältöjä ilman lupaa eteenpäin esimerkiksi alihankkijoilleen? | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 28. mikä on toimittajan vastuu järjestelmästä löytyvistä virheistä ja tietoturva-aukoista?                                                                                                                                                                                                                                   | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 29. että toimittaja ei saa käyttää omassa muussa toiminnassaan oman organisaatiosi omistamia tietosisältöjä kuten asiakastietoja (esim. kaupallisessa tarkoituksessa)?                                                                                                                                                       | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |
| 30. onko sopimuksessa määritelty tilaajan mahdollisuus auditoida tai käyttää kolmatta osapuolta auditoidessa toimittajan toimintaa tietoturva- ja tietosuoja-asioden toteutuksessa ja kuinka auditoinnin kustannukset on jaettu?                                                                                             | <input type="checkbox"/> Kyllä<br><input type="checkbox"/> Ei |