Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.	
15 § Vahingoilta suojaaminen	versio 0.9/01.11.2019

15.1 § Vahingoilta suojaaminen

Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:
2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;

Hallituksen esitys HE 284/2018
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Viranomaisella tulisi olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä ja vahingoilta kuten tulipalot, vesivahingot tai ilkivalta tai sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta kuten laitteiden rikkoutuminen. Tietoa tai järjestelmää tulee suojata asianmukaisin, mutta riskiarvioinnin perusteella oikeasuhtaisen toimin. Lisätietoja järjestelmän vaikutusten ja riskien arvioinnista kortissa 13 § Riskienhallinta.

Viranomaisen tulisi määrittää kullekin tietoaineistolle hyväksytyt sijainnit, joissa sähköisessä ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä ja myös säilyttää. Sijaintien määrittämisessä pitää huomioida palveluiden toteuttamistapa, kuten palveluntuottajat, pilvipalvelut, sekä tiedon käsittelyn fyysinen sijainti.

Tyypillisesti palvelutarjoajat säilyttävät ja ylläpitävät tietojen ja tietojärjestelmien käsittelyssä tarvittavia fyysisiä tiloja ja laitteita. Tällöin palveluntarjoajien kanssa on sovittava fyysisen turvallisuuden vaatimusten toteutumisesta. Viranomaisen tulee varmistua siitä, että palvelutarjoaja täyttää säädetyt sekä riskiarvioinnin perusteella asetetut vaatimukset. Lisätietoja tietoturvallisuuteen liittyvistä vaatimuksista löytyy tämän ohjeen lopussa viitatusta VAHTI 2/2014 Tietoturvallisuuden arviointiohjeesta. Viranomaisen tulee huomioida, että järjestelmän tai tiedon mahdollinen turvallisuusluokittelu aiheuttaa myös vaatimuksia palveluntarjoajaa ja/tai viranomaista kohtaan.

Viranomaisen tulee huomioida tiedon ja tietojärjestelmien fyysisen turvallisuuteen liittyen seuraavat seikat:

- Rakenteellinen turvallisuus: Tilojen rakenteiden tulee täyttää niihin kohdistuvat suojaustasovaatimukset jotka perustuvat säilytettävän tiedon tai tietojärjestelmien turvallisuusluokitukseen. Lisätietoja rakenteellisista vaatimuksista löytyy Kansallisen auditointi kriteeristön F-osiosta.
- Turvallisuusvyöhykkeet: Mikäli tiloissa säilytettävään tietoon kohdistuvat vaatimukset sitä edellyttävät, tulee toimitilat olla jaettu turvallisuusvyöhykkeisiin, joiden tarkoituksena on estää tai riittävästi hidastaa oikeudettomien tahojen pääsy käsiksi tietoon tai tietojärjestelmään.
- Pääsynhallinta: Vain henkilöillä joilla on työtehtäviin perustuva oikeus käsitellä tiloissa säilytettävää tietoa tai tietojärjestelmää tulee olla pääsy näihin. Muiden tahojen pääsy tulee estää kulunvalvonnalla tai muulla vastaavalla ratkaisulla, jolla voidaan estää tai havaita asiaton pääsy ja reagoida riittävällä nopeudella.
- Olosuhdevalvonta: Tiloissa tulee olla säilytettävän tiedon ja tietojärjestelmä vaatimuksiin nähden riittävä olosuhdevalvonta esimerkiksi tulipalon, vesivahingon, kaasuvuodon, pölyn, tärinän varalle.
- Varavoima & UPS: Tietojärjestelmillä tulisi olla käytössä UPS-ratkaisu yllättävien virtapiikkien tai sähkökatkosten varalta, joka mahdollistaa järjestelmän toiminnan siksi ajaksi kunnes se voidaan ajaa hallitusti alas ja siirtyä jatkuvuussuunnitelman mukaiseen toimintaan.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua, tietoon kohdistuvien riskien tunnistaminen, arviointi ja asianmukainen hallinta.

15 § Vahingoilta suojaaminen	versio 0.9/01.11.2019

Lisätietoja toimitilaturvallisuuteen liittyvistä vaatimuksista ja ohjeistuksista löytyy VAHTI 2/2013 – Toimitilojen tietoturvaohjeesta.

Kriittiset järjestelmät tulisi kahdentaa, niin että toimintaa voidaan jatkaa toisesta konesalista tai sijainnista käsin vaikka toiminta ensisijaisessa ylläpitosijainnissa olisi estynyt. Tietoaineistojen osalta tulee huomioida tiedon turvallisuusluokittelun kautta tulevat tiedon käsittely ja säilytysvaatimukset ja toteuttaa nämä asianmukaisesti.

Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi huomioida vahingoilta suojaamisessa:

- Täyttääkö palveluntarjoaja tietoturvallisuusvaatimukset fyysisen turvallisuuden osalta kun on huomioitu käsiteltävän tiedon turvallisuusluokittelu tai tietojärjestelmän kriittisyys?
- Onko pääsy tiloihin rajattu vain niihin henkilöihin joilla on oikeus käsitellä tietoja?
- Onko kriittiset järjestelmät kahdennettu siten että toimintaa voidaan jatkaa mikäli ensisijainen ylläpitosijainti ei ole käytössä?
- Mikäli viranomainen ylläpitää tietojärjestelmiä itse, onko tietojen turvallisuusluokituksesta ja/tai järjestelmän kriittisyydestä johtuvat vaatimukset huomioitu ja täytetty?
    - Onko fyysiset tilat rajattu turvallisuusvyöhykkeisiin?
    - Ovatko tilojen rakenteelliset ratkaisut riittävät?
    - Onko tiloissa olosuhdevalvonta tulipalon ja kosteusvaurioiden varalle?
    - Onko käytössä varavoimaratkaisu joka takaa järjestelmän riittävän toiminnan hallitun alasajon ajaksi?

Kortti 13 § Riskienhallinta

Kansallinen auditointi kriteeristö Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaiselle
Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)
VAHTI 2/2014 – Tietoturvallisuuden arviointiohje
VAHTI 2/2013 – Toimitilojen tietoturvaohje
VAHTI 2/2012 – ICT-varautumisen vaatimukset