**LIITE 3**

**Valitse mitä suojatoimia tutkimuksessasi käytetään riskien vähäentämiseksi ja torjumiseksi.**

 **(rastita ja/tai kuvaile käytössä oleva suojatoimi)**

**TEKNISIÄ SUOJATOIMIA**

**Työasemien hallinta (valitse)**

[ ]  **a)** Käytössä on IT-palvelujen tarjoama **työsema**

* Käyttäjillä ei ole oletuksena ylläpito-oikeuksia.
* IT-palvelujen kautta hankitun XXX-ohjelmiston käyttöön ei tarvita ylläpito-oikeuksia.
* Windowsin Autorun-toiminnallisuus on estetty (USB-tikut, CD- ja DVD-levyt).
* Langaton eduroam-verkko on määritelty käyttöön IT-palvelujen asennusohjelmalla tai ohjeilla, mikä estää hyökkäykset verkkoyhteyden tunnistukseen ja salaukseen.

[ ]  **b)** Käytössä on IT-palvelujen tarjoama **kovennettu tutkimustietokone/työasema**

* IT-palvelujen tarjoamien kovennettujen tutkimuskoneiden / työasemien langaton UTU Staff -verkko on määritelty IT-palvelujen toimesta estämään hyökkäykset tunnistukseen ja salaukseen.

[ ]  **c)** Käytössä on **muu tietokone tai työasema**, jonka hallinnasta on huolehdittu seuraavasti (kuvaile): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**IT-laitteistojen ja palvelimien käyttöturvallisuus esim. päivitys ym. (valitse)**

[ ]  **a)** Käytössä on yliopiston IT-palvelujen tarjoama **työasema ja palvelin tai kovennettu tutkimustietokone**

* IT-palvelujen tarjoamiin työasemiin ja palvelimiin asennetaan keskitetysti päivitykset keskeisimpiin tietoturvan kannalta tärkeisiin 3. osapuolen sovelluksiin (esim. Adobe Flash Player, Oracle Java, Adobe Acrobat Reader, Mozilla Firefox). Päivitykset asentuvat automaattisesti mikäli koneelle ei kukaan ole kirjautunut sen ollessa päällä. Koneelle kirjautunut käyttäjä voi valita milloin päivitykset asennetaan.
* IT-palvelujen tarjoamalle kovennetulle tutkimuskoneelle / henkilökohtaisille työasemille Windows- ja Office-päivitykset tulevat asennettavaksi 2 vrk kuluttua Microsoftin julkaisusta. Päivitykset asentuvat automaattisesti mikäli koneelle ei kukaan ole kirjautunut sen ollessa päällä. Koneelle kirjautunut käyttäjä voi valita milloin päivitykset asennetaan.

[ ]  **b)** Tutkimusta tehdään **myös** käyttäen IT-palvelujen ylläpitämien **IT-luokkien työasemia**

* IT-palvelujen ylläpitämiin IT-luokkiin ja muihin jaettuihin työasemiin Windows- ja Office-päivitykset asennetaan automaattisesti 2 vrk kuluttua Microsoftin julkaisusta.

[ ]  **c)** Käytössä on IT-palvelujen tarjoama **Windows-palvelin**

* IT-palvelujen tutkimusprojektille tarjoamille Windows-palvelimille päivitykset asennetaan 2 päivän päästä tai seuraavassa huoltoikkunassa mikäli siitä on erikseen sovittu.

[ ]  **d)** Käytössä on IT-palvelujen tutkimusprojekteille tarjoama **RHEL-palvelin**

* IT-palvelujen tutkimusprojektille tarjoamille RHEL-palvelimille tietoturvapäivityksiä asennetaan kerran vuorokaudessa tai seuraavassa huoltoikkunassa mikäli siitä on erikseen sovittu. Kernel-päivitykset otetaan käyttöön huoltoikkunoissa.

[ ]  **e)** Käytössä on **muu laite tai palvelin**, jossa päivitys on hoidettu seuraavasti (kuvaile): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**IT-laitteiden tai työasemien huolto (valitse)**

[ ]  **a)** Käytössä on IT-palvelujen tarjoama **työasema tai kovennettu tutkimustietokone**

* IT-palvelujen tarjoamien työasemien huolto tapahtuu tyypillisesti on-site-palveluna laitevalmistajan huollon toimesta IT-palvelupisteen tiloissa.
* Projektilevyjen tallennusjärjestelmän vialliset levyt tuhotaan tai tyhjennetään EU-alueella.
* IT-palvelut ylläpitää tarjoamiaan kovennettuja tutkimuskoneita / työasemia keskitetysti.

[ ]  **b)** Käytössä on **muu laitteisto**, jonka huolto hoidetaan seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Laitteiden turvallinen tyhjentäminen ennen niiden hävittämistä (valitse)**

[ ]  **a)** Käytössä on **yliopiston laitteet.**

* IT-palveluiden käyttämä SER-palvelu huolehtii laitteiden tietoturvallisesta hävittämisestä.
* Asiakkaalla on myös Leasing-sopimuksissa oikeus pitää tallennusmediat itsellään
* Kovennettujen tutkimuskoneiden data voidaan tuhota hävittämällä BitLocker-avain.
* IT-palvelujen tarjoaman turvatulostuksen kautta tulostettujen töiden data-alue ylikirjoitetaan heti tulostamisen jälkeen.

[ ]  **b)** Käytössä on **muu laitteisto**, jonka turvallinen tyhjentäminen hoidetaan seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verkon turvallisuus (valitse)**

[ ]  **a)** Käytetään **yliopiston tiloissa yliopiston tarjoamia** **työasemia ja verkkoja.**

* Yliopiston tiloissa IT-palvelujen tarjoamat työasemat liitetään ensisijaisesti joko Ethernet-lähiverkkoon tai langattomaan UTU Staff –verkkoon. Nämä yliopiston työasemille tarjotut verkot on eristetty Internetistä palomuurilla, joka ei oletuksena salli pääsyä työasemille Internetistä ja tyypillisesti sallii eri verkkoalueiden välillä vain tarpeellisen liikenteen. IT-palvelujen tarjoamat työasemat ovat pääasiassa erotettu palomuurilla henkilökohtaisista laitteista, mutta tutkimustarpeisiin henkilökohtaisia työasemia voi olla samoissa verkoissa IT-palvelujen tarjoamien työasemien kanssa.
* Lähiverkon suojausratkaisut vaihtelevat rakennuksittain. Viimeksi tekniikaltaan päivitettyjen kohteiden osalta käytössä on IEEE 802.1X –porttitunnistus laitteiden ja käyttäjien tunnistamiseen sekä rajoituksia lähiverkon väärinkäytön varalta.
* Langaton UTU Staff –verkko käyttää vahvaa salausta (WPA2 Enterprise) sekä laitteiden tunnistusta (EAP-TLS). Laitteiden välinen liikenne on estetty.
* Langaton eduroam-verkko käyttää vahvaa salausta (WPA2 Enterprise) sekä laitteiden tai käyttäjien tunnistusta (EAP-TLS ja EAP-PEAP). Laitteiden välinen liikenne on estetty.
* Eduroam-asetukset on asennettu IT-palvelujen tarjoamasta asennuspaketista, joka estää kirjautumiset muille kuin yliopiston omalle tunnistuspalvelimelle.

[ ]  **b)** IT-palveluilta on tilattu **erillinen palomuurilla suojattu aliverkko** tutkimusprojektin tarpeisiin.

[ ]  c**)** Käytössä on **muu verkko**, jonka turvallisuudesta huolehditaan seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verkon toiminnan valvonta (valitse)**

[ ]  **a)** Tutkimusta tehdään käyttäen **yliopiston verkkoa**.

* IT-palvelut valvoo yliopiston järjestelmien ja verkon käyttöä. Tietoturvajärjestelystä JulkL 24.1 § 7 k

[ ]  **b)** Tutkimusta tehdään pääasiallisesti käyttäen **muuta verkkoa**, jonka valvontaa on järjestetty seuraavasti:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Haittaohjelmistoilta suojautuminen (valitse)**

[ ]  **a)** Käytössä on IT-palvelujen tarjoama **henkilökohtainen työasema ja yliopiston verkko.**

* IT-palvelujen tarjoamissa henkilökohtaisissa työasemissa käyttäjillä ei oletuksena ole ylläpito-oikeuksia, mikä rajoittaa haittaohjelmien toimintamahdollisuuksia. Erillisiä ylläpito-oikeudellisilla käyttäjätunnuksia käytetään vain niitä vaativiin erikoistoimiin.
* Yliopiston työasemille tarjoamat verkot on eristetty Internetistä palomuurilla, joka ei oletuksena salli pääsyä työasemille Internetistä. IT-palvelujen tarjoamat työasemat ovat pääasiassa erotettu palomuurilla henkilökohtaisista laitteista, mutta tutkimustarpeisiin henkilökohtaisia työasemia voi olla IT-palvelujen tarjoamien työasemien kanssa samoissa verkoissa.

[ ]  **b)** Käytössä on IT-palvelujen tarjoama **kovennettu tutkimuskone/työasema**

* IT-palvelujen tarjoamissa kovennetuissa tutkimuskoneissa / työasemissa palomuuri estää sisään tulevat yhteydet ja siten estää lähiverkon ja Internetin kautta tarttuvia haittaohjelmia. Liikenne IT-palvelujen ylläpitopalvelimilta on sallittu rajatusti.
* IT-palvelujen tarjoamissa kovennetuissa tutkimuskoneissa / työasemissa on antivirus-ohjelmisto, joka käyttää useita tekniikoita työaseman suojaamiseen haittaohjelmilta.
* IT-palvelujen tarjoamissa kovennetuissa tutkimuskoneissa ja jaetuissa työasemissa käyttäjillä ei ole ylläpito-oikeuksia, mikä rajoittaa haittaohjelmien toimintamahdollisuuksia.

[ ]  **c)** Käytössä on IT-palvelujen tutkimusprojektille tarjoama **palvelin**

* IT-palvelujen tutkimusprojektille tarjoamat palvelimet on liitetty yliopiston palomuurin suojaamaan DMZ-verkkoon, johon sallitaan pääsy Internetistä vain erikseen pyydetyille palveluille ja oletuksena pääsy palvelimelle Internetistä on estetty.

[ ]  **d)** Käytössä on **muita laitteita**, jotka on suojeltu haittaohjelmistoilta seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pääsynvalvonta IT-laitteisiin (valitse)**

[ ]  **a)** Käytössä on Turun yliopiston **utu-tunnus**.

* Turun yliopiston käyttäjätunnuksen salasana on voimassa 190 päivää, vähimmäispituus 10 merkkiä ja se muodostetaan isoista ja pienistä aakkosista, numeroista ja ASCII-erikoismerkeistä. Salasanassa ei saa olla käyttäjän käyttäjätunnusta, etunimeä tai sukunimeä.

[ ]  **b)** Käytössä on **kovennettu tutkimuskone**

* Pääsy IT-palvelujen tarjoamille kovennetuille tutkimuskoneille on rajattu sovittuihin yliopiston keskitetyn käyttäjähallinnan tunnuksiin ja kovennettuihin tutkimuskoneisiin. IT-palvelujen työasemaylläpito käyttää määrittelyihin Microsoft Active Directoryn työkaluja.
* Kovennetun tutkimuskoneen ylläpito-oikeudet on rajoitettu siten, että koneen administrator-oikeudet ovat vain erikseen määriteltyjen henkilöiden tiedossa.

[ ]  **c)** Käytössä on **muita laitteita**, joiden pääsynvalvonta on hoidettu seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Varmuuskopiot (valitse)**

[ ]  **a)** Data on tallennettu/varmuuskopioitu IT-palvelujen tarjoamalle **projektivelvylle**

* Data on tallennettu / varmuuskopioitu IT-palvelujen tarjoamalle projektilevylle, joka on hajautettu kahteen IT-palvelujen konesaliin Turun seudulla. Projektilevyistä säilytetään snapshotit 26 viikon ajan ja niistä säilytetään suojakopiota toisessa konesalissa 2 viikon ajan, ellei IT-palvelujen kanssa ole muuta sovittu.

[ ]  **b)** Data on tallennettu/varmuuskopioitu IT-palvelujen tarjoamalle **Taltio-levylle**

* Tallennettu data replikoidaan kolmeen IT-palvelujen Turun seudulla sijaitsevaan konesaliin hajautettuun tallennusklusteriin. Datasta otetaan kerran viikossa (viikonloppuisin) read-only snapshot, joista neljä uusinta säilytetään (eli neljän viikon snapshotit).

[ ]  **c)** Data on tallennettu/varmuuskopioitu IT-palvelujen tarjoamaan **Seafile-pilvitallenukseen**

* Seafileen tallennettu data replikoidaan kolmeen IT-palvelujen Turun seudulla sijaitsevaan konesaliin hajautettuun tallennusklusteriin. Konesalit ovat IT-palvelujen hallinnassa Turun seudulla.. Seafile ylläpitää snapshotien sijaan tiedostoille omaa sisäistä versiointiaan, joka säilyttää vanhoja versioita oletuksena 90 päivää (käyttäjä voi itse muokata säilytysaikoja kirjastokohtaisesti).

[ ]  **d)** Tallennus tehdään **muulla tavalla**. Varmuuskopiointi on hoidettu seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verkkosivujen turvallisuus (valitse)**

[ ]  **a)** Käytössä on **yliopiston verkkosivut.**

* + Yliopisto soveltaa Kyberturvallisuuskeskuksen ja Viestintäviraston ohjeistusta.

[ ]  **d)** Käytössä on **muut verkkosivut.** Turvallisuus hoidetaan seuraavasti (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Jäljitettävyys eli lokit (valitse jos on käytössä)**

[ ]  **a)** Käytössä on it-palvelujen **virtuaalipalvelin**

* Tutkimusprojektin IT-palveluilta hankkiman virtuaalipalvelimen XXX-lokit säilytetään kaksi vuotta.

[ ]  **b)** Käytössä on **itsenäisesti tai IT-palvelujen kautta hankittu tietokoneohjelma**, joka kerää lokitietoja. Kuvaile lokitietojen toiminta: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Salaus (valitse)**

[ ]  **a) Käytetään yliopisto tarjoamia verkkoja ja noudatetaan yliopiston ohjeita verkkojen käyttämisestä**

* Yliopistolla käytetään vahvasti salattuja langattomia eduroam- ja UTU Staff -verkkoja.
* Sähköpostiviestintä hoidetaan yliopiston sähköpostijärjestelmällä, joka käyttää tietoliikenneyhteyksissä vahvaa salausta.
* Julkisissa verkoissa käytetään IT-palvelujen tarjoamaa vahvasti salattua VPN-yhteyttä.

[ ]  **b) Kovennettu tutkimuskone**

* Dataa käsitellään IT-palvelujen tarjoamalla kovennetulla tutkimuskoneella, jonka kiintolevy on salattu BitLocker-salauksella ja jonka käyttö on rajattu tutkimusprojektin osallistuville henkilöille. BitLocker vaatii PIN-koodia jokaisella koneen käynnistyskerralla ja koneella ei ole käytössä muistinvaraista sleep-tilaa.

[ ]  **c) Seafile-tallennuspaikkana**

* Data on tallennettu/varmuuskopioitu IT-palvelujen ylläpitämän Seafile-pilvitallennuspalvelun salasanalla suojattuun ja vahvasti salattuun kirjastoon.

[ ]  **d) Yliopiston virtuaalipalvelin**

* Tutkimusprojektin IT-palveluilta hankkiman virtuaalipalvelimen tietoliikenne hoidetaan vahvasti salatuilla SSH- ja HTTPS-yhteyksillä. HTTPS-salauksessa käytetään vahvaa ja julkisesti luotettua DigiCert-varmennetta.

[ ]  **e)** Käytössä lisäksi **muu salaus** (kuvaile):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Sivustakatselusuoja (valitse, jos käytössä)**

[ ]  Käytössä on IT-palveluilta on tilattu henkilökohtaisen työaseman näyttöön sivustakatselusuoja.

**Paperiasiakirjojen suojaus (valitse)**

[ ]  **a)** Tutkimuksessa kerättävien paperiasiakirjojen suojaus (säilyttäminen, tuhoaminen jne,) hoidetaan seuraavasti: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  **b)** Tutkimuksessa ei synny henkilötietoja sisältäviä paperiasiakirjoja

**Fyysinen pääsynvalvonta (valitse)**

[ ]  **a)** Tutkimusta tehdään yliopiston tiloissa, joissa fyysinen kulunvalvonta on järjestetty seuraavasti (esim. kulkuluvat, lukitut ovet jne.): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  **b)** Tutkimusta tehdään muualla. Fyysinen pääsynvalvonta henkilötietoihin on hoidettu seuraavasti (kuvaile): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ORGANISATORISIA SUOJATOIMIA**

**Tietosuojapolitiikka**

Tutkimuksen henkilötietojen käsittelyssä sovelletaan Yliopiston hallituksen 16.2.2018 hyväksymää tietosuojapolitiikkaa.

**Tutkimusta suorittavien ohjeistus**

Tutkimuksesta vastaava: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ huolehtii siitä, että

[ ]  Kaikille tutkimusta suorittaville henkilöille (työntekijöille, apurahatutkijoille, opiskelijoille jne.) on annettu henkilötietojen käsittelyä koskevaa ohjeistusta ja ohjausta.

[ ] Tutkimusta suorittavat ovat sitoutuneet noudattamaan yliopiston ohjeita saadessaan käyttöönsä utu-tunnuksen.

[ ]  Kun tutkimusta suorittava jättää tehtävänsä, häneltä poistetaan oikeus käyttää utu-tunnusta eli hänellä ei enää ole mahdollisuutta käyttää yliopiston järjestelmiä.

**Käsittelijöiden ohjeistus**

Tutkimuksesta vastaava: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ huolehtii siitä, että

[ ]  Kaikkien käsittelijöiden (palveluntarjoajien ja muiden yhteistyökumppanien) kanssa on tehty 28 artiklan mukainen sopimus tai muu asiakirja.

**Käsittelyoikeuksien rajoittaminen**

Tutkimuksesta vastaava: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ huolehtii siitä, että

[ ]  Käyttäjäprofiilein tai muulla tavoin huolehditaan siitä, että käyttöoikeudet henkilötietoihin on rajoitettu vain niitä tarvitseville.

[ ]  Peruutetaan tutkimusta suorittavien, rekisterinpitäjän lukuun toimivien käsittelijöiden ja kolmansien osapuolten käyttöoikeudet, kun heillä ei enää ole oikeutta käyttää tiloja tai resurssia tai kun heidän sopimuksensa tai muu oikeutensa käyttää tietoja päättyy.

**Valvonta**

Turun yliopisto on nimennyt tietosuojavastaavan, joka seuraa ja valvoo yliopistossa yleisesti tietosuoja-asetuksen noudattamista.

Tutkimuksesta vastaava \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ valvoo ja arvioi näiden suojaustoimien tehokkuutta ja riittävyyttä.

**Henkilötietoja koskevien tietomurtojen hallinta**

Tutkimuksesta vastaava: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ huolehtii siitä, että

[ ] Henkilötietoja käsittelevät ohjeistetaan toimimaan yliopiston ohjeiden mukaisesti tietomurron tapahtuessa.

* Tutkimusta suorittava ilmoittaa havaitsemastaan tietoturvapoikkeamasta tietoturva@utu.fi –palveluosoitteeseen, joka jatkaa asian käsittelyä.
* Yliopistolla on tietoturvapoikkeamien käsittelyyn turvallisuusorganisaatio ja IT-palveluissa poikkeamien havaitsemiseen ja käsittelyyn CSIRT-organisaatio (Computer Security Incident Response Team). Tietosuojakysymyksissä mukaan kytketään myös tietosuojavastaava.

**KÄSITTELYYN LIITTYVIÄ SUOJATOIMIA**

**Henkilötietojen määrän minimointi**

[ ] Henkilötietojen käsittelyyn liittyviä riskejä on pyritty lieventämään rajoittamalla käsittelyä mm. suodattamalla, poistamalla, arkaluontoisuuden vähentämisellä konversion avulla, tietojen tunnistettavuuden vähentämisellä, tietojen kertymisen rajoittamisella, tietojen käyttöoikeuden rajoittamisella ym. (kuvaile miten/mitkä keinot ovat käytössä): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Aineiston pseudonymisointi (kuvaile)**

[ ]  Aineisto pseudonymisoidaan seuraavasti (kuvaile missä vaiheessa ja miten): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**MUITA KÄYTETTÄVIÄ SUOJATOIMIA**

**Lisäksi käytetään seuraavia suojatoimia**: (kuvaile tässä muut mahdollisesti käytettävät suojatoimet):

[ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_