2016

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Lapin yliopiston tietoturvapolitiikka

Vahvistettu Lapin yliopiston rehtorin päätöksellä 16.5.2016

Lapin yliopiston tietoturvapolitiikka

Sisällysluettelo:

1. Johdanto

Tietoturvapolitiikka on Lapin yliopiston rehtorin vahvistama sisäinen toimintatapamääräys, joka jaetaan tiedoksi ja noudatettavaksi koko henkilöstölle. Tietoturvapolitiikan periaatteita noudatetaan myös Lapin yliopiston yhteistyökumppaneiden kanssa tehtävissä sopimuksissa sekä sidosryhmien käyttäjille laadittavissa ohjeissa.

Tätä tietoturvapolitiikkaa täydentävät erikseen laaditut käyttö- ja ylläpito-ohjeet ja se tulee huomioida kaikessa Lapin yliopiston ohjeistuksessa.

2. Tietoturvapolitiikan tavoite

Lapin yliopistossa tietototurvallisuuden ensisijaisena päämääränä on Lapin yliopiston vastuulla olevien palveluiden jatkuvuuden turvaaminen.

Toimintalähtöisesti painottuvalla tietoturva-asioiden hoidolla tuetaan Lapin yliopiston ydintoiminnoille asetettuja vaatimuksia.

2.1. Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Se edellyttää tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali-, että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuus on toimintatapa, jonka tavoitteena on tietojärjestelmien ja toiminnan jatkuvuutta uhkaavien riskien hallinta. Se on edellytys Lapin yliopiston ydintoimintojen hoitamiselle.

2.2. Määritelmät

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:

Luottamuksellisuus: tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.

Eheys: tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus sekä ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys: ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Todentaminen (autentikointi): varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta ja alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.

Kiistämättömyys; tietoverkossa eri menetelmin saatava näyttö siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi.

3. Tietoturvatoimintaa ohjaavat tekijät

Tietoturvatoimintaa ohjataan säädöksin, ohjein ja suosituksin. Tärkeimmät Lapin yliopiston toimintaa tietoturvallisuuden ja tietosuojan näkökulmasta ohjaavat säädökset ovat yliopistolaki ja -asetus, hallintolaki, yhteistoimintalaki, henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta, laki sähköisestä asioinnista viranomaistoiminnassa, laki yksityisyyden suojasta työelämässä ja tietoyhteiskuntakaari sekä Lapin yliopiston johtosääntö.

4. Tietoturvallisuuteen kohdistuvat uhat

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Henkilöiden mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys aiheuttavat merkittävän uhan Lapin yliopiston tietoturvallisuudelle. Lisäksi uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, tekniset ongelmat sekä Lapin yliopistolle palveluita tuottavien ulkopuolisten palveluiden tarjoajien toimet.

5. Tietoturvallisuuden merkitys organisaatiolle

Lapin yliopiston operatiivinen toiminta on huomattavan tieto- ja järjestelmäriippuvaista. Siitä syystä tietoriskien hallintaan tulee kiinnittää erityistä huomiota.

5.1. Toiminnan kannalta elintärkeät palvelutehtävät ja turvattavat kohteet

Lapin yliopiston toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan.

Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen verkon toiminnan turvaaminen sekä palveluiden tuottaminen Lapin yliopiston sidosryhmille ja palveluiden tuottajille.

5.2. Tietoturvaperiaatteet

Tietojenkäsittelyn turvaamisperiaatteita ovat ennaltaehkäisy, turvatoimien ajantasainen seuranta ja kehittäminen sekä tietojärjestelmien toiminnan ja käytön valvonta.

Lapin yliopiston tietojärjestelmien määrittely-, suunnittelu- ja toteutusvaiheissa on huomioitava mahdolliset järjestelmien käyttöön kohdistuvat riskit ja varauduttava niiden ennaltaehkäisyyn. Toteutusvaiheessa varmistetaan tarkoituksenmukaiset suojausmenettelyt, jolloin järjestelmien käyttäjillä on tietotarpeita vastaava käyttöympäristö. Periaatteena Lapin yliopistossa on tietojärjestelmien tietojen käytön salliminen vain työtehtävien hoitamiseen, kumppaneilla sopimusten ja lupien mukaisten tehtävien hoitamiseen.

5.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Toiminnan jatkuvuus tulee turvata jatkuvuussuunnittelulla, joka sisältää häiriöiden ennalta estämisen ja mahdollistaa niistä nopean toipumisen.

Tietojärjestelmien turvasuunnitelmissa, -järjestelyissä ja -ohjeissa varaudutaan tietoturvallisuutta koskevien laiminlyöntien, vahinkojen tai virheiden jälkikäteisselvittämiseen periaatteena kustannusten kohtuullisuus saatuun hyötyyn nähden. Periaatteet toteutetaan tietoturvasuunnitelmassa kuvatulla tavalla.

6. Turvatoimien priorisointi

Lapin yliopiston turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

- henkilön hengen tai terveyden turvaaminen
- arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen
- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen.

7. Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, joka koostuu mm. seuraavista toimintamalleista ja dokumenteista:

- tietoturvapolitiikka,
- tietoturvakäytännöt ja -periaatteet,
- tietoturvallisuuden kehittämissuunnitelma,
- tietoturvallisuuden perus- ja lisäohjeistus,
- tietoturvakoulutus,
- tietoturvapoikkeamien käsittely,
- tietoturvaraportointi johdolle,
- jatkuvuus- ja valmiussuunnitelmat,
- toimintaan liittyvät tietoturvaprosessit sekä
- auditointisuunnitelma.

Hallintajärjestelmä toteuttaa Lapin yliopiston strategiaa ja strategian toimeenpanosuunnitelmaa. Se kattaa tietoturvallisuuden yksityiskohtaisen organisoinnin, politiikat, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit. Sen avulla myös seurataan ja arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa valmiuksia hallita tietoturvallisuutta systemaattisesti.

8. Tietoturvavastuut

8.1. Organisaation tietoturvavastuut

Tietoturvallisuuden kehittäminen on jatkuvaa laaja-alaista toimintaa, jossa eri vastuuhenkilöryhmillä on omat tehtävänsä.

Tietoturvatoiminnassa noudatetaan Lapin yliopiston hallintoyksikön työjärjestyksen mukaista organisointia ja vastuunjakoa. Tulosyksiköt vastaavat tietoturvallisuuden toteutumisesta omalla vastuualueellaan.

Tietoturvatoiminnan ja tietoturvallisuuden hallintajärjestelmän kehittämisestä vastaa Lapin yliopiston tietohallinto-organisaatio ja Lapin korkeakoulukonsernin palvelukeskuksen IT-palvelualue Lapin yliopiston tietoturvapäällikön johdolla.

Yksityiskohtaiset vastuut on kuvattu Lapin yliopiston tietoturvavastuudokumentissa.

8.2. Organisaation yhteistyökumppaneiden vastuut

Lapin yliopistolle palveluita tuottavat yritykset tulee velvoittaa nimeämään yritykseen tietoturvayhteyshenkilö, joka vastaa Lapin yliopiston ohjeistaman tietoturvatason noudattamisesta yrityksessä. Kumppaneille asetettavat tietoturvavaatimukset on kuvattu kunkin sopimuksen erillisessä liitteessä.

9. Tietoturvakoulutus ja –ohjeet

Tietoturvallisuus on sisällytetty Lapin yliopiston perehdytysprosessiin. Tietoturvakoulutusta järjestetään kaikille työntekijöille määräajoin.

Tietoturvaohjeistuksen sisällöstä ja ajantasaisuudesta vastaa tietoturvapäällikkö.

Kumppaneille laaditaan erillistä tietoturvaohjeistusta ja tietoturva-asiat sisällytetään kumppaneille järjestettävään koulutukseen.

10. Tietoturvallisuudesta tiedottaminen

Tietoturva-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaa tietoturvapäällikkö yhdessä Viestintäpalveluiden kanssa.

Viestintäpalvelut ovat vastuussa Lapin yliopiston ulkoisesta tiedottamisesta. Tietoturva-asioista ei aktiivisesti tiedoteta yliopiston ulkopuolelle, mutta jos tiedottamistarvetta ilmenee, se hoidetaan kuten muukin ulkoinen tiedottaminen.

11. Tietoturvallisuuden toteutumisen valvonta

Jokainen Lapin yliopiston henkilöstöön kuuluva on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä ICT-palvelupisteen kautta. Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin tulosyksikkö tai Lapin yliopistolle palveluja tuottava yritys omalla vastuualueellaan.

Lapin yliopiston tietoturvapolitiikan toteutumista seuraa tietoturvapäällikkö, joka raportoi siitä tietohallintojohtajalle.

12. Toiminta poikkeustilanteissa ja –oloissa

Poikkeusoloissa toimitaan Lapin yliopiston valmiussuunnitelman menettelytapojen mukaisesti.

Poikkeusolojen toiminnan suunnittelusta vastaa hallintojohtaja.