LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Vahvistettu Lapin yliopiston rehtorin päätöksellä 14.09.2022

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 yhteistyökumppaneiden kanssa tehtävissä sopimuksissa sekä sidosryhmien käyttäjille laadittavissa ohjeissa.

2. Tietoturvapolitiikan tavoite

Tietoturvallisuuden ensisijaisena päämääränä on turvata toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, pyrkiä estämään tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedontuhoutuminen tai vääristyminen.

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.

Tietoturvallisuuden kehittäminen ja ylläpito ovat osa yleistä turvallisuustoimintaa ja riskien hallintaa.

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

Tietoturvallisuudesta huolehditaan kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti sekä noudattaen tietoturvallisuuden parhaita käytäntöjä ja suosituksia.

4. Tietoturvallisuuteen kohdistuvat uhat

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

Uhkia aiheuttavat mm. tietomurrot, virheellisesti toimivat ohjelmistot, tietojärjestelmät ja laitteet, tekniset ongelmat sekä ulkopuolisten palveluiden tarjoajien toimet. Myös käyttäjien mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys voivat aiheuttaa uhan tietoturvallisuudelle.

5. Tietoturvallisuuden merkitys organisaatiolle

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

5.1. Toiminnan kannalta elintärkeät palvelutehtävät ja turvattavat kohteet

Tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan.

5.2. Tietoturvaperiaatteet

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

Tietojärjestelmien ja -palvelujen määrittely-, suunnittelu- ja toteutusvaiheissa huomioidaan mahdolliset järjestelmien tai palvelujen käyttöön kohdistuvat riskit ja varaudutaan niiden ennaltaehkäisyyn. Toteutusvaiheessa varmistetaan tarkoituksenmukaiset suojausmenettelyt, jolloin järjestelmien ja palvelujen käyttäjillä on tietotarpeita vastaava käyttöympäristö.

5.3. Tietoturvallisuuden sopeuttaminen avoimeen kansainväliseen toimintaan

Tietoturvallisuuden tason määrittämisessä voi hyödyntää alan kansainvälisiä standardeja. Tietoturvallisuuden tavoitteiden asettelussa, mittaamisessa ja turvamekanismien valinnassa käytetään hyväksi kansainvälisiä ja kansallisia standardeja ja suosituksia ja niissä omaksuttua terminologiaa.

Kansainvälistymistä tuetaan tarjoamalla tietoturvallisuuteen liittyvää aineistoa ja koulutusta tarvittaessa myös englanninkielisinä.

5.4. Tietoturvallisuuden tuki tutkimukselle, opetukselle ja yhteistyölle

Tietoturvallisuuden tavoitteena on mahdollistaa tutkimuksen, opetuksen ja yhteistyön tarvitsemien tiedon käsittely- ja kommunikointimenetelmien turvallinen ja tehokas käyttö. Turvatoimet skaalautuvat yksittäisen tutkijan tai opettajan tasolta tutkimusprojektien ja -ryhmien, opintojaksojen, oppiaineiden ja yksiköiden kautta koko organisaatiota koskeviksi.

5.5. Tietoturvallisuuden tuki hallinnolle ja muille tukitoiminnoille

Tietoturvallisuudesta huolehditaan osana hallinnon järjestelmä- ja prosessikehitystä. Tietoturvatoimilla pyritään edistämään uusien ja tehokkaiden järjestelmien ja toimintatapojen käyttöönottoa kaikissa toiminnoissa.

5.6. 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

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.

8. Tietoturvavastuut

8.1. Sisäiset tietoturvavastuut

Lapin yliopiston tietoturvallisuudesta vastaa yliopiston rehtori. Teknisestä tietoturvallisuudesta vastaa LUC IT-palvelut. Tieto- ja digipalvelujen johtaja vastaa tietoturvallisuuden kehittämisestä ja seurannan toteuttamisesta sekä tietoturvallisuutta koskevasta ulkoisesta yhteistyöstä. Yliopiston kokonaisturvallisuudesta ja ennakoinnista vastaava työryhmä sekä IT-johtoryhmä valmistelevat tietoturvallisuuden kehittämistoimenpiteitä.

Jokainen Lapin yliopistolainen on vastuussa tietoturvallisuuden toteutumisesta omassa toiminnassaan ja on myös velvollinen ilmoittamaan tietoturvallisuudessa havaitsemistaan puutteista.

8.2. Palvelutoimittajien vastuut

Palvelutoimittajien kanssa tietoturvavaatimukset ja vastuut määritellään sopimuksin.

9. Tietoturvatietoisuuden kehittäminen

Tietoturvallisuus on sisällytetty henkilökunnan perehdytysprosessiin. Henkilöstön tietoturvatietoisuutta pyritään kehittämään koulutuksin sekä kulloinkin ajankohtaisin tiedottein ja ohjein.

Tietoturvaohjeistuksen sisällöstä ja ajantasaisuudesta huolehditaan muuttuvan toimintaympäristön mukaan.

10. Tietoturvallisuudesta tiedottaminen

Tietoturva-asioista tiedotetaan henkilöstöä tarpeen mukaan. Henkilöstölle tiedottaminen hoidetaan Tietohallinto ja IT-palvelut yksikön toimesta.

Tietoturva-asioista ei aktiivisesti tiedoteta yliopiston ulkopuolelle, mutta jos tiedottamistarvetta ilmenee, se hoidetaan ulkoisen viestinnän periaatteiden mukaisesti.