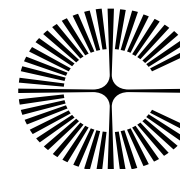


# Tietoturvapolitiikka

Tarkoitus ja tavoitteet	Periaatteet	Tietoturvan toteuttaminen
<ul style="list-style-type: none"><li>Tietoturvapolitiikka määrittelee tietojen turvaamisen tavoitteet, periaatteet, vastuut ja toteutuskeinot</li><li>Tavoitteena on:<ul style="list-style-type: none"><li>Varmistaa toimintaympäristön ja -tapojen <u>riittävä ja tarkoituksenmukainen</u> turvallisuus sekä häiriötön toiminta</li><li>Varmistaa toiminnan jatkuvuus normaalioloissa sekä häiriö- tai poikkeustilanteissa</li><li>Tiedon suojaamisen varmistaminen (luottamuksellisuus)<ul style="list-style-type: none"><li>Tietoihin luvattoman pääsyn estäminen</li></ul></li><li>Tiedon oikeellisuuden takaaminen (eheys)<ul style="list-style-type: none"><li>Tiedon vääristymisen estäminen</li></ul></li><li>Tiedon käytettävyyden ja saatavuuden mahdollistaminen siltä osin, kun on tarpeen (käytettävyys)<ul style="list-style-type: none"><li>Tiedon tuhoutumisen estäminen</li><li>Tietoihin pääsyn varmistaminen tarpeen mukaan</li></ul></li><li>Toiminnalle tärkeiden tietojärjestelmien, palveluiden ja tietoverkkojen turvaaminen</li><li>Tietoturvakulttuurin kehittäminen ja sen kautta parantanut tietoturvallisuuden taso</li></ul></li></ul>	<ul style="list-style-type: none"><li>Toiminnan ydinprosessit ja kriittiset tiedot on määritetty ja turvattu</li><li>Tietoturvatointa perustuu riskienhallintaan</li><li>Tietoturvatointia ohjaavat lainsäädäntö sekä tämä tietoturvapolitiikka ja sitä täydentävä dokumentaatio</li><li>Avoimuus tietoturvaloukkauksien ilmoittamisessa</li><li>Jokainen Careerian työntekijä ja opiskelija on velvollinen noudattamaan tätä tietoturvapolitiikkaa ja sitä täydentäviä ohjeistuksia ja käytänteitä</li><li>Tämän politiikan vastaisesta toiminnasta aiheutuvat seuraukset määräytyvät Careerian yleisen kurinpitomenettelyn mukaisesti</li><li>Tietoturvallisuuteen liittyvä vastuunjako on kuvattu tämän politiikan Tietoturvallisuuden vastuut –liitedokumentissa</li></ul> <p><b>Opiskelijat ja heidän henkilötietonsa ovat tärkeimpiä suojattavia asioita</b></p>	<ul style="list-style-type: none"><li>Toiminta perustuu jatkuvaan kehittämiseen, jossa tarkoituksena on tuoda tietoturva osaksi jokaisen päivittäistä toimintaa ja toimintatapoja</li><li>Tietoturvariskejä hallitaan säännöllisellä ja järjestelmällisellä riskienhallinnalla, jonka avulla kohdistetaan toimintaa kriittisyyden mukaan</li><li>Jatkuvuus- ja valmiussuunnittelu kohdennetaan Careerian kriittisiin toimintoihin ja prosesseihin sekä niitä toteuttaviin tai tukeviin tietojärjestelmiin</li><li>Tietojen luokittelumenetelmän avulla ohjeistetaan tavat tietojen luokittelulle sekä määritellään tietoturvakontrollit eri luokkiin kuuluvan tiedon käsittelylle</li><li>Sopimuskumppaneille määritetään riittävät tietoturva vaatimukset</li><li>Henkilöstön ja opiskelijoiden tietoturvaosaamista ja –tietoisuutta parannetaan säännöllisillä koulutuksilla, ajantasaisilla ja selkeillä ohjeilla sekä aktiivisella tietoturva-asioiden viestinnällä</li><li>Tietoturvallisuutta seurataan ja valvotaan<ul style="list-style-type: none"><li>Ulkoisilla auditoinneilla</li><li>Sisäisillä tarkastuksilla ja katselmuksilla</li><li>Teknistä tietoturvallisuutta seurataan myös jatkuvalla ja osittain automaattisella valvonnalla</li></ul></li><li>Tietoturvapoikkeamien ilmoittamiseen kannustetaan ja poikkeamiin reagoidaan asianmukaisesti. Poikkeamia hallitaan määritellyn prosessin mukaisesti.</li><li>Mahdollisista tietoturvaloukkauksista tiedotetaan aktiivisesti ja asianmukaisesti sisäisesti sekä tarvittaessa ulkoisesti.</li><li>Tarkemmat tietoturvan toteuttamisen keinot on määritelty tätä tietoturvapolitiikkaa täydentävässä dokumentaatioissa</li><li>Henkilötietojen käsittelyyn liittyvät asiat on kuvattu tarkemmin Careerian tietosuojapolitiikassa</li></ul>

**TIETOTURVAPOLITIikka ON HYVÄKSYTTY JOHTORYHMÄSSÄ (11.10.2021) JA SE ON VOIMASSA TOISTAISEKSI. SE ON ASIAKIRJANA JULKINEN JA SAATAVISSA CAREERIAN VERKKOSIVUILTA**



**CAREERIA**