					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P03					Asiakirjan nimi: **Hyväksyttävän käytön politiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyn kanssa

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 5	Määrittää käyttäytymisnormit ja hyväksyttävän käytön politiikkaa koskevat vaatimukset
ISO/IEC 27002:2022	Kontrollit 6.1, 6.2, 8.1, 8.12	Ohjaa tietoturvavastuita, tietoisuutta sekä laitteiden ja tietojen hallintaa
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	IT-varojen käyttöön liittyvät käytönhallinnan sekä tietoisuuden ja käyttäytymisen kontrollit
EU:n GDPR	Artiklat 5(1)(f), 32; johdanto-osan kappale 39	Edellyttää luottamuksellisuutta ja eheyttä, teknisiä ja organisatorisia toimenpiteitä sekä asianmukaista oikeusperustaa käytölle
EU:n NIS2-direktiivi	Artikla 21(2)(a–d)	Edellyttää operatiivisia politiikkoja ja turvallista käyttöä koskevaa koulutusta
EU:n DORA-asetus	Artikla 5	Tukee ICT-riskienhallintaa säätelemällä käyttäjätoimintaa
COBIT 2019	APO07, BAI05, DSS05, MEA01	Henkilöstöresurssit, muutoksenhallinta, hallitut turvallisuuspalvelut sekä vaatimustenmukaisuuden ja suorituskyvyn seuranta

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation tietojärjestelmien, laskentaresurssien, viestintävälineiden ja tietojen käsittelykäytäntöjen sallitun ja kielletyn käytön.

1.2 Se varmistaa, että kaikki käyttäjät ymmärtävät vastuunsa käyttäessään organisaation IT-varoja ja että heidän toimintansa tukee tietojen luottamuksellisuutta, eheyttä, saatavuutta ja lainmukaista käsittelyä.

1.3 Tämä politiikka täyttää ISO/IEC 27001:2022 -standardin kohdan 5.10 vaatimuksen määrittämällä järjestelmien käyttöä koskevat käyttäytymisnormit ja ottamalla käyttöön teknisiä ja menettelyllisiä suojatoimia väärinkäytön, huolimattomuuden tai virheellisen käytön riskin minimoimiseksi.

1.4 Se tukee myös tutkinta- ja täytäntöönpanotoimenpiteitä, mukaan lukien poikkeamien hallinta ja rikkomuksiin liittyvät kurinpidolliset toimenpiteet.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan kaikkiin henkilöihin ja tahoihin, joille on myönnetty pääsy organisaation tietojärjestelmiin ja varoihin, mukaan lukien seuraavat:

2.1.1 Työntekijät, alihankkijat, konsultit, harjoittelijat ja vuokratyöntekijät

2.1.2 Kolmannet osapuolet, joilla on järjestelmän käyttöoikeus tai delegoitu hallinnollinen rooli

2.1.3 Vieraat tai kumppanit, jotka käyttävät organisaation omistamaa tai hyväksymää IT-infrastruktuuria

2.2 Soveltamisalaan kuuluvat kaikki organisaation teknologia- ja tietovarat, mukaan lukien:

2.2.1 Työasemat, kannettavat tietokoneet, mobiililaitteet ja palvelimet

2.2.2 Verkkoinfrastruktuuri ja pilvipalvelut

2.2.3 Sähköposti, viestintäpalvelut, tiedostotallennus, yhteistyöalustat ja VPN-yhteydet

2.2.4 Lepotilassa olevat, siirrettävät tai käsiteltävät tiedot niiden muodosta tai sijainnista riippumatta

2.2.5 Kaikki henkilökohtaiset laitteet, joita käytetään BYOD-järjestelyn (Bring Your Own Device) mukaisesti ja jotka yhdistetään organisaation järjestelmiin

2.3 Tätä politiikkaa sovelletaan kaikissa työympäristöissä, mukaan lukien:

2.3.1 Toimistot ja tuotantotoimipaikat

2.3.2 Etätyöympäristöt ja hybridityöjärjestelyt

2.3.3 Kenttätoiminnot tai kolmansien osapuolten hallinnoimat toimitilat

2.4 Kaikkien käyttäjien on vahvistettava politiikan vastaanotto ja noudatettava sitä ehtona organisaation järjestelmien käyttöoikeudelle tai organisaation tietojen käsittelylle.

3. Tavoitteet

3.1 Määrittää ja toimeenpanna organisaation IT-resurssien hyväksyttävää käyttöä koskevat säännöt.

3.2 Estää luvaton pääsy, tietovuodot ja vahingot, jotka johtuvat huolimattomasta tai haitallisesta käytöstä.

3.3 Suojata organisaation verkkoja, varoja ja tietoja käyttäjätoiminnasta aiheutuvilta uhkilta.

3.4 Tukea lakisääteisten ja sopimusvelvoitteiden täyttämistä osoittamalla asianmukaista huolellisuutta IT-resurssien hallinnoinnissa.

3.5 Varmistaa yhdenmukaisuus ja selkeys kurinpidollisten toimenpiteiden ja poikkeamien hallintaprosessien soveltamisessa.

3.6 Edistää eettisen, turvallisen ja vastuullisen digitaalisten ja fyysisten laskentaresurssien käytön kulttuuria.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy hyväksyttävän käytön politiikan (AUP) ja varmistaa, että se on linjassa liiketoimintatavoitteiden, sääntelyvaatimusten ja organisaation arvojen kanssa.

4.1.2 Osoittaa resurssit politiikan toimeenpanoon, koulutukseen, seurantaan ja katselmointiin.

4.1.3 Katselmoi vaatimustenmukaisuuden tilan ja politiikan rikkomuksiin liittyvät kurinpidolliset toimenpiteet osana tietoturvallisuuden hallintajärjestelmän ohjausta.

4.2 IT- ja tietoturvatiimit

4.2.1 Toteuttavat tekniset suojatoimet tämän politiikan toimeenpanemiseksi, mukaan lukien:

4.2.2 Sisällönsuodatus, haittaohjelmasuojaus, päätelaitehallinta ja verkon valvontatyökalut

4.2.3 Sähköpostin tietoturva-asetukset ja tiedonvuodon estoratkaisut (DLP)

4.2.4 Estolistat ja sallittujen kohteiden listat ohjelmistoille, laitteistoille ja verkkosivustoille

4.2.5 Ylläpitävät luetteloa hyväksytyistä ja kielletyistä ohjelmistoista, laitteista ja palveluista.

4.2.6 Tutkivat epäiltyjä AUP-rikkomuksia, keräävät digitaalista todistusaineistoa ja tukevat tarvittaessa kurinpidollisia tai oikeudellisia toimenpiteitä.

4.2.7 Tekevät yhteistyötä henkilöstöhallinnon ja lakiasioiden kanssa poikkeamien käsittelyssä, eskaloinnissa ja ilmoitusvelvoitteiden täyttämisessä.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Katselmoinnin käynnistävät tekijät ja tiheys

9.1.1 Tämä politiikka on katselmoitava:

9.1.1.1 Vähintään kerran vuodessa

9.1.1.2 Merkittävien teknologia- tai infrastruktuurimuutosten jälkeen

9.1.1.3 Sellaisten poikkeamien tai auditointihavaintojen jälkeen, jotka osoittavat puutteita toimeenpanossa

9.1.1.4 Sovellettavan lainsäädännön tai sopimusten muuttuessa

9.2 Omistajuus ja hyväksyntä

9.2.1 CISO tai nimetty tietoturvallisuuden hallintajärjestelmän vastuuhenkilö vastaa katselmointiprosessista.

9.2.2 Päivitykset on hyväksyttävä ylimmässä johdossa ja viestittävä koko organisaatiolle.

9.2.3 Päivitettyjen ehtojen hyväksyntä on kerättävä uudelleen politiikan uudelleenjulkaisun yhteydessä.

9.3 Asiakirjahallinta

9.3.1 Politiikan on sisällettävä seuraavat metatiedot ja versiointitiedot:

9.3.1.1 Otsikko, tunniste ja luokittelutaso

9.3.1.2 Politiikan omistaja ja asiakirjasta vastaava henkilö

9.3.1.3 Muutoshistoria ja päivitysten perustelut

9.3.1.4 Katselmointipäivä ja seuraavan suunnitellun päivityksen ajankohta

9.3.1.5 Jakelu- ja hyväksyntälokin viitteet

9.3.2 Pääversio on säilytettävä tietoturvallisuuden hallintajärjestelmän asiakirjarekisterissä versionhallittuna.

10. Liitännäiset politiikat ja yhteydet

10.1 Tätä politiikkaa on tulkittava yhdessä seuraavien politiikkojen kanssa:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää hyväksyttävään käyttöön liittyvät perustavanlaatuiset käyttäytymisodotukset ja ylimmän johdon sitoutumisen.

10.1.2 P4 – Käytönhallintapolitiikka: Määrittää käyttäjiin, järjestelmiin ja tietojen käyttöön liittyvät oikeudet ja valtuudet sekä toimeenpanee suoraan hyväksyttävän käytön rajat.

10.1.3 P6 – Riskienhallintapolitiikka: Käsittelee käyttäytymiseen liittyviä riskejä ja tukee käyttäjälähtöisiin uhkiin liittyvää seurantaa ja riskien käsittelyä.

10.1.4 P7 – Perehdytys- ja päättämispolitiikka: Varmistaa, että hyväksyttävän käytön ehdot hyväksytään palvelussuhteen alussa ja käyttöoikeudet poistetaan sen päättyessä.

10.1.5 P9 – Etätyöpolitiikka: Laajentaa hyväksyttävän käytön vaatimukset etä- ja hybridityöympäristöihin.

10.2 Nämä liitännäiset politiikat muodostavat kerroksellisen puolustusmallin käyttäytymisen, teknisten kontrollien ja sopimuksellisen hallinnoinnin näkökulmasta.

11. Viitestandardit ja viitekehykset

11.1 Tämä hyväksyttävän käytön politiikka (AUP) on yhdenmukaistettu kansainvälisesti tunnustettujen standardien ja oikeudellisten viitekehysten kanssa, jotta kaikessa digitaalisten ja fyysisten tietojärjestelmien käytössä varmistetaan toimeenpantavat, todennettavat ja riskiperusteiset käyttäytymiskontrollit.

11.2 ISO/IEC 27001:2022

11.2.1 Kohta 5.10 – Tiedon ja muiden siihen liittyvien varojen hyväksyttävä käyttö: Tämä politiikka täyttää suoraan vaatimuksen määrittää, viestiä ja toimeenpanna IT-resurssien asianmukaista käyttöä koskevat säännöt.

11.2.2 Liite A, kontrolli 6.1 – Tietoturvallisuuden vastuut: Määrittää selkeät vastuut käyttäjätoiminnalle ja vaatimustenmukaisuuden valvonnalle.

11.2.3 Liite A, kontrolli 6.2 – Tietoturvatietoisuus, koulutus ja opastus: Koulutus ja politiikan hyväksymisprosessit ovat osa AUP:n toimeenpanoa.

11.2.4 Liite A, kontrolli 8.1 – Käyttäjän päätelaitteet ja 8.12 – Tiedonvuodon estäminen: Kattaa käyttäjälaitteilla noudatettavan hyväksyttävän toiminnan ja hallitsee toimia, jotka voivat johtaa tietojen paljastumiseen tai vuotamiseen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (mobiililaitteiden käytönhallinta) ja AC-20 (ulkoisten tietojärjestelmien käyttö): Tämä politiikka määrittää käyttäjien velvollisuudet ja rajoitukset BYOD-järjestelyille ja kolmansien osapuolten järjestelmäkäytölle.

11.3.2 PL-4 (käyttäytymissäännöt): Tarjoaa yksityiskohtaiset hyväksyttävän käytön vaatimukset, jotka ovat tämän politiikan mukaisia.

11.3.3 AT-2 (tietoturvatietoisuuden koulutus): Toteutetaan käyttäjäkoulutuksen ja dokumentoidun politiikan hyväksynnän kautta.

11.3.4 AU-2 (auditointitapahtumat) ja AU-12 (auditointitietojen tuottaminen): Toimeenpano perustuu käyttäjätoimien seurantaan ja rikkomuksista hälyttämiseen.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 5(1)(f): Edellyttää henkilötietojen turvallisuutta ja eheyttä; tämä politiikka vähentää inhimillisestä toiminnasta ja luvattomasta käytöstä aiheutuvia riskejä.

11.4.2 Artikla 32: Edellyttää teknisiä ja organisatorisia toimenpiteitä, kuten käyttäytymiskontrolleja ja käyttörajoituksia, henkilötietojen suojaamiseksi.

11.4.3 Johdanto-osan kappale 39: Korostaa tarvetta varmistaa, että vain valtuutetuilla henkilöillä on tarpeellinen pääsy tietoihin ja että tietoja käytetään lainmukaisesti.

11.5 EU:n NIS2-direktiivi (2022/2555):

11.5.1 Artikla 21(2)(a–d): Edellyttää operatiivisia politiikkoja ja koulutusta järjestelmien turvalliseen käyttöön, minkä tämä AUP toteuttaa määrittämällä käyttäytymisen, seurannan ja toimeenpanoprosessit.

11.6 EU:n DORA-asetus (2022/2554):

11.6.1 Artikla 5: Tämä politiikka tukee ICT-riskienhallinnan viitekehystä määrittämällä ihmisen ja järjestelmän vuorovaikutusta koskevat säännöt ja minimoimalla käyttäytymiseen perustuvaa kyberriskialtistusta.

11.7 COBIT 2019:

11.7.1 APO07 – Hallitut henkilöstöresurssit: Toimeenpanee käyttäjävastuut ja tietoisuuden koko työsuhteen elinkaaren ajan.

11.7.2 BAI05 – Hallittu organisaatiomuutos: Sisällyttää hyväksyttävän käytön hallinnoinnin käyttäjätoimintaan vaikuttaviin muutoksiin.

11.7.3 DSS05 – Hallitut turvallisuuspalvelut: Tukee käyttäjätoiminnan seurantaa, käyttäytymishälytyksiä ja automatisoituja reagointimekanismeja.

11.7.4 MEA01 – Suorituskyvyn ja vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: Tämä politiikka määrittää mittarit ja mekanismit käyttäjien käyttäytymisodotusten noudattamisen varmentamiseksi.