					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P07S					Asiakirjan nimi: **Perehdytys- ja työsuhteen päättämispolitiikka**							
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**

Standardien ja säädösten viitekehys

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 6.2, 7	Henkilöstöturvallisuuden ja tietoisuuden vaatimukset
ISO/IEC 27002:2022	Kontrollit 6.2, 6.5	Perehdytyksen ja työsuhteen päättämisen tietoturvakäytännöt
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Työsuhteen päättäminen, tilien elinkaaren hallinta ja suunnittelu
EU:n NIS2-direktiivi	Artikla 21(2)(h)	Henkilöstöturvallisuus ja käyttöoikeuksien elinkaaren hallinta
EU:n DORA-asetus	Artikla 12	Käyttövalvonta ja käyttöoikeuksien peruminen ICT-järjestelmissä
COBIT 2019	APO07, DSS01	Henkilöstöturvallisuus sekä loogisen ja fyysisen pääsyn hallinta
EU:n GDPR	Artikla 32	Henkilötietojen turvallisuus työsuhteen aikana

1. Tarkoitus

1.1 Tämä politiikka määrittää menettelyt uusien työntekijöiden ja sopimuskumppanien perehdyttämiselle sekä käyttöoikeuksien turvalliselle poistamiselle, kun henkilö poistuu organisaatiosta tai vaihtaa roolia.

1.2 Se varmistaa, että käyttöoikeudet myönnetään vain työtehtävien edellyttämässä laajuudessa vähimmän oikeuden periaatteen mukaisesti, kaikki omaisuuserät ovat jäljitettävissä ja kriittiset toimenpiteet, kuten järjestelmien käytöstäpoisto ja tietojen palautus, toteutetaan viipymättä.

1.3 Tämä politiikka tukee vaatimustenmukaisuutta, toiminnan eheyttä ja tietosuojaa jäsennellyillä ja todennettavilla perehdytys- ja työsuhteen päättämistoimilla.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin vakituisiin ja määräaikaisiin työntekijöihin

2.1.2 sopimuskumppaneihin, konsultteihin ja harjoittelijoihin

2.1.3 ulkoisiin palveluntarjoajiin, joilla on järjestelmä- tai fyysinen pääsy

2.2 Politiikka kattaa seuraavat:

2.2.1 perehdytys: käyttäjätilien perustaminen, käyttöoikeuksien myöntäminen ja laitteiden luovutus

2.2.2 poistumismenettely: käyttöoikeuksien poistaminen, yrityksen omaisuuden palautus sekä digitaalisten identiteettien turvallinen sulkeminen

2.2.3 sisäiset roolimuutokset, jotka edellyttävät käyttöoikeuksien uudelleenmäärittelyä tai omaisuuserien uudelleenkohdentamista

2.3 Politiikka koskee kaikkia laitteita, alustoja ja sijainteja, joita käytetään viralliseen liiketoimintaan.

3. Tavoitteet

3.1 Varmistaa, että uusi henkilöstö saa käyttöoikeudet ja resurssit varmennettujen roolien ja vastuiden perusteella.

3.2 Varmistaa, että poistuvien käyttäjien pääsy järjestelmiin ja toimitiloihin poistetaan kokonaan viimeistään heidän viimeisen työpäivänsä päättyessä.

3.3 Estää orvot käyttäjätilit ja palauttamatta jääneet omaisuuserät, jotka muodostavat tietoturvariskin.

3.4 Ylläpitää dokumentoidut tiedot perehdytykseen, sisäisiin siirtoihin ja poistumismenettelyihin liittyvistä toimista.

3.5 Edistää vastuun osoitettavuutta tarkistuslistojen ja poikkitoiminnallisen roolikoordinoinnin avulla.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Hyväksyy etuoikeutettujen käyttäjäroolien käyttöoikeudet ja valvoo perehdytys- ja työsuhteen päättämisohjelmaa.

4.1.2 Varmistaa, että poikkeukset ovat perusteltuja ja että korjaavat toimenpiteet toteutetaan, jos menettelyjä ei noudateta.

4.2 Toimistopäällikkö / henkilöstöhallinto

4.2.1 Käynnistää uusien työntekijöiden perehdytyksen ja ilmoittaa IT:lle lähtijöistä.

4.2.2 Varmistaa, että oikeudelliset asiakirjat (esim. salassapitosopimus (NDA)) ja tietoturvapolitiikkojen kuittaukset on suoritettu.

4.2.3 Ylläpitää perehdytys- ja työsuhteen päättämisen tarkistuslistoja sekä seuraa politiikan noudattamista.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Vuosittainen katselmointi

9.1.1 Tämä politiikka on katselmoitava vähintään kerran vuodessa toimitusjohtajan sekä henkilöstöhallinnon ja IT:n vastuuhenkilöiden toimesta.

9.2 Katselmoinnin aikaistavat herätteet

9.2.1 Päivitykset on tehtävä, jos:

9.2.1.1 otetaan käyttöön uusia henkilöstöhallinnon tai IT-järjestelmiä

9.2.1.2 ulkoinen IT-palveluntarjoaja tai ulkoistettu HR-palvelu vaihtuu

9.2.1.3 tietoturva-auditoinnit paljastavat prosessipuutteita

9.2.1.4 sääntelyvelvoitteet muuttuvat (esim. EU:n GDPR:n päivitykset)

9.2.1.5 tapahtuu kriittinen poistumismenettelyn epäonnistuminen tai tietomurto

9.3 Versionhallinta ja hyväksyntä

9.3.1 Tämän politiikan jokaisen version on sisällettävä:

9.3.1.1 versionumero ja päivämäärä

9.3.1.2 yhteenveto muutoksista

9.3.1.3 toimitusjohtajan hyväksyntä

9.3.1.4 arkistoidut aiemmat versiot, joita säilytetään vähintään kolme vuotta

9.4 Viestintä ja kuittaus

9.4.1 Kaikille perehdytyksestä tai työsuhteen päättämisestä vastuussa oleville työntekijöille on tiedotettava politiikan päivityksistä. Vuosittaiset tietoisuus- tai kertauskoulutukset ovat pakollisia.

10. Liittyvät politiikat ja yhteydet

10.1 Tämä politiikka tukee seuraavia politiikkoja, ja sitä tukevat seuraavat politiikat:

10.1.1 P2S – Hallintoroolien ja -vastuiden politiikka: varmistaa vastuun osoitettavuuden käyttöoikeus- ja perehdytysprosesseissa

10.1.2 P4S – Käyttövalvontapolitiikka: määrittää roolipohjaisen käyttöoikeuksien myöntämisen ja käytöstäpoiston teknisen toteutuksen

10.1.3 P6S – Riskienhallintapolitiikka: arvioi riskit, jotka aiheutuvat perehdytys- ja työsuhteen päättämiskontrollien epäonnistumisesta

10.1.4 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: asettaa henkilöstön perehdytysvaatimukset työsuhteen alussa

10.1.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: käsittelee käyttöoikeuksien poistamatta jättämisen tai omaisuuden varkauden tietoturvapoikkeamina

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Kohta 6.2 – Määrittää henkilöstöturvallisuuden vaatimukset

11.1.2 Kohta 7.2 – Edellyttää tietoisuuskoulutusta uudelle henkilöstölle

11.2 ISO/IEC 27002

11.2.1 Kontrollit 6.2 ja 6.5 – Kuvaavat perehdytykseen ja työsuhteen päättämiseen liittyvät tietoturvakäytännöt

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Työsuhteen päättämismenettelyt, mukaan lukien käyttöoikeuksien käytöstäpoisto

11.3.2 AC-2 – Varmistaa käyttäjätilien elinkaaren hallinnan

11.3.3 PL-4 – Edellyttää henkilöstösiirtymien suunnittelua

11.4 EU:n GDPR

11.4.1 Artikla 32 – Varmistaa asianmukaisen turvallisuuden työsuhteen aikana ja sen jälkeen erityisesti henkilötietojen käyttöoikeuksien osalta

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(h) – Edellyttää henkilöstöturvallisuuden ja käyttöoikeuksien elinkaaren hallintakeinoja

11.6 EU:n DORA-asetus

11.6.1 Artikla 12 – Edellyttää säännellyiltä finanssialan toimijoilta henkilöstön ICT-järjestelmien käyttöoikeuksien hallintaa, mukaan lukien käyttöoikeuksien perumismenettelyt

11.7 COBIT 2019

11.7.1 APO07 – Henkilöstöresurssien hallinta: määrittää henkilöstön elinkaareen liittyvät tietoturvavaatimukset

11.7.2 DSS01 – Toimintojen hallinta: kattaa loogisen ja fyysisen pääsyn hallinnan työsuhteen siirtymätilanteissa