					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P07					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**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/säädös	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Clause 7.2, Clause 6	Henkilöstön pätevyys, turvallinen perehdyttäminen sekä työsuhteen päättämiseen tai muutoksiin liittyvien vastuiden toimeenpano.
ISO/IEC 27002:2022	Controls 6.2, 6.5, 5	Perehdytykseen, käyttöoikeuksiin ja henkilöstön elinkaaren hallintaan liittyvät hallintakeinot.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Henkilöstösiirrot ja työsuhteen päättäminen, vähimmän oikeuden periaate, auditointilokitus sekä käyttöoikeuksien hallinta henkilöstömuutosten aikana ja niiden jälkeen.
EU:n GDPR	Articles 5(1)(f), 25, 32; Recital 39	Käyttöoikeuksien rajaaminen, luottamuksellisuus, suojaus sekä henkilötietojen asianmukaiset hallintakeinot.
EU:n NIS2-direktiivi	Article 21(2)(b, c, d)	Henkilöstöön ja toimintaan liittyvät tietoturvatoimenpiteet, sisäpiiriuhkien hallinta sekä elinkaariprosessit.
EU:n DORA-asetus	Articles 5, 8, 9	Hallinnointi, sisäinen ICT-valvonta, ICT-riskienhallinta ja poikkeamien hallinta henkilöstösiirtymien aikana.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Henkilöstöhallinto, tiedonhallinta, tietoturva ja vaatimustenmukaisuus perehdytyksen ja työsuhteen päättämisen yhteydessä.

1. Tarkoitus

1.1 Tämä politiikka määrittää yhdenmukaiset menettelyt perehdytyksen, sisäisten siirtojen ja työsuhteen päättämisen hallintaan kaikille käyttäjäryhmille.

1.2 Politiikka varmistaa fyysisen ja loogisen pääsyn, käyttäjätilien oikea-aikaisen ja turvallisen perustamisen sekä käytöstäpoiston, luottamuksellisuuden, vastuun osoitettavuuden ja omaisuuden palautuksen.

1.3 Tämä politiikka vähentää luvattomaan pääsyyn, tietovuotoihin ja palauttamatta jääneeseen omaisuuteen liittyviä riskejä sisällyttämällä perehdytys- ja työsuhteen päättämisen hallintakeinot henkilöstöhallinnon, IT:n ja tietoturvan prosesseihin.

1.4 Tämä politiikka tukee ISO/IEC 27001:2022 -standardin liitteen A hallintakeinoa 6.5 varmistamalla, että henkilöstöturvallisuuteen liittyviä velvoitteita sovelletaan työsuhteen tai toimeksiannon aikana ja sen päättymisen jälkeen.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia työntekijöitä, urakoitsijoita, konsultteja, toimittajia ja muita kolmansia osapuolia, joille myönnetään pääsy organisaation järjestelmiin, verkkoihin, toimitiloihin tai tietoihin.

2.2 Tämä politiikka kattaa koko seuraavan elinkaaren:

2.2.1 Perehdytys (rekrytointi, sopimussuhteen alkaminen tai määräaikainen toimeksianto)

2.2.2 Sisäiset siirrot tai roolimuutokset

2.2.3 Poistumisprosessi (irtisanoutuminen, eläköityminen, työsuhteen päättäminen, sopimuksen päättyminen)

2.3 Politiikka kattaa:

2.3.1 Loogisen pääsyn (järjestelmät, sovellukset, pilvipalvelut, VPN)

2.3.2 Fyysisen pääsyn (kulkutunnisteet, avaimet, rakennusten kulunvalvontajärjestelmät)

2.3.3 Osoitetut omaisuuserät (kannettavat tietokoneet, puhelimet, pääsytunnisteet, tunnistetiedot)

2.3.4 Politiikkojen kuittauksen ja salassapitovelvoitteet

2.4 Kaikki toiminnot (henkilöstöhallinto, IT, toimitila- ja omaisuudenhallinta, tietoturva ja johto) vastaavat oman roolinsa toteuttamisesta perehdytys- ja poistumisprosessin työnkuluissa.

3. Tavoitteet

3.1 Varmistaa, että käyttöoikeuksia myönnetään vasta sen jälkeen, kun tietoturvaan, koulutukseen ja sopimusvaatimuksiin liittyvät edellytykset on täytetty.

3.2 Perua käyttöoikeudet ja palauttaa organisaation omaisuus välittömästi roolin muuttuessa tai työsuhteen päättyessä.

3.3 Säilyttää organisaation omaisuuden luottamuksellisuus, eheys ja saatavuus henkilöstösiirtymien aikana.

3.4 Tukea auditoitavuutta ja oikeudellista puolustettavuutta kattavilla tallenteilla perehdytys- ja työsuhteen päättämistapahtumista.

3.5 Vähentää sisäpiiriuhkien riskiä varmistamalla ja dokumentoimalla kaikki henkilöstöön liittyvät käyttöoikeustapahtumat.

3.6 Yhdenmukaistaa henkilöstön elinkaaren hallinta riskiperusteisten tietoturvakäytäntöjen ja sääntelyvaatimusten kanssa.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy tämän politiikan ja osoittaa toimivallan sekä resurssit perehdytys-, poistumis- ja pääsynhallintaprosesseille.

4.1.2 Varmistaa, etteivät henkilöstösiirtymät altista organisaatiota kohtuuttomalle tietoturva- tai oikeudelliselle riskille.

4.2 Henkilöstöhallinto

4.2.1 Käynnistää työntekijöiden perehdytys- ja työsuhteen päättämisen työnkulut sekä ilmoittaa muutoksista asiaankuuluville toiminnoille.

4.2.2 Varmistaa, että taustatarkastukset, sopimukset, salassapitosopimus (NDA) ja politiikan kuittaus on suoritettu ennen käyttöoikeuksien myöntämistä.

4.2.3 Ilmoittaa IT:lle sekä toimitila- ja omaisuudenhallinnalle henkilöstön lähdöistä ilmoitusten palvelutasosopimuksen mukaisesti.

4.2.4 Tekee yhteistyötä laki- ja vaatimustenmukaisuustoiminnon kanssa työsuhteen jälkeisten velvoitteiden (esim. salassapitolausekkeiden) soveltamiseksi.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Politiikan katselmointitiheys

9.1.1 Tämä politiikka on katselmoitava:

9.1.1.1 Vuosittain, tai

9.1.1.2 Merkittävän käyttöoikeuksien väärinkäyttöön, omaisuuden menetykseen tai menettelyvirheeseen liittyvän poikkeaman jälkeen

9.1.1.3 Toteutettaessa merkittäviä muutoksia henkilöstöhallinnon tai IAM-alustan osalta

9.1.1.4 Henkilötietoihin tai velvoitteisiin vaikuttavien sääntely- tai lakimuutosten yhteydessä

9.2 Katselmointiprosessi ja omistajuus

9.2.1 ISMS-päällikön ja henkilöstöjohtajan on koordinoitava katselmointi IT-tietoturvan sekä laki- ja vaatimustenmukaisuustoiminnon tuella.

9.2.2 Kaikki muutokset on hyväksyttävä ylimmän johdon ja ISMS-ohjausryhmän toimesta.

9.2.3 Päivitetyt versiot on jaettava uudelleen asianomaisille toiminnoille ja henkilöstölle uudelleenkuittausta varten.

9.3 Asiakirjahallinta ja säilytys

9.3.1 Tämän politiikan on sisällettävä:

9.3.2 Versionhallinta, muutoshistoria ja voimaantulopäivä

9.3.3 Vastuutettu omistaja ja katselmoija(t)

9.3.4 Politiikan luokitus ja hyväksyntätallenne

9.3.5 Vanhentuneet versiot on arkistoitava vähintään kolmeksi vuodeksi asiakirjahallintapolitiikan mukaisesti.

10. Liittyvät politiikat ja yhteydet

10.1.1 Tämä politiikka integroidaan suoraan seuraaviin:

10.1.2 P1 – Tietoturvapolitiikka: Määrittää organisaation tietoturvatavoitteet, mukaan lukien henkilöstön käyttöoikeuksien hallinnan.

10.1.3 P4 – Käyttövalvontapolitiikka: Määrittää operatiiviset vaatimukset järjestelmä- ja fyysisen pääsyn myöntämiselle sekä käyttöoikeuksien perumiselle perehdytys- ja työsuhteen päättämisherätteiden perusteella.

10.1.4 P3 – Hyväksyttävän käytön politiikka: Edellyttää kuittausta perehdytyksen yhteydessä ja tukee soveltamista työsuhteen päättymisen jälkeen.

10.1.5 P6 – Riskienhallintapolitiikka: Varmistaa, että käyttäjäkäyttöoikeuksiin ja siirtymiin liittyvät riskit arvioidaan ja käsitellään ISMS-periaatteiden mukaisesti.

10.1.6 P11 – Käyttäjätilien ja käyttöoikeuksien hallintapolitiikka: Määrittää tätä politiikkaa tukevat käyttäjätilien perustamisen ja käytöstäpoiston tekniset hallintakeinot.

10.2 Nämä politiikat muodostavat integroidun hallintajärjestelmän henkilöstön elinkaaritapahtumien turvalliseen ja vastuulliseen hallintaan.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukaistettu kansainvälisesti tunnustettujen tietoturvan, tietosuojan ja IT-hallinnoinnin viitekehysten kanssa, jotta perehdytys- ja työsuhteen päättämisprosessit ovat turvallisia, jäljitettäviä ja lakisääteisten sekä organisaation vaatimusten mukaisia.

11.2 ISO/IEC 27001:

11.2.1 Lauseke 7.2 – Pätevyys ja lauseke 6.2 – Tietoturvatavoitteet: Tämä politiikka tukee henkilöstön pätevyyden varmistamista ja henkilöiden turvallista perehdyttämistä rooleihin, joissa he vaikuttavat ISMS:n tavoitteisiin.

11.2.2 Liitteen A hallintakeino 6.5 – Vastuut työsuhteen päättymisen tai muutoksen jälkeen: Tämä politiikka toimeenpanee täysimääräisesti hallintakeinot, jotka koskevat jäljelle jääviä käyttöoikeuksia, tietojen hallussapitoa ja sopimusvelvoitteita henkilön lähtiessä.

11.2.3 Liitteen A hallintakeino 5.9 – Taustatarkastukset ja 6.2 – Työsuhteen ehdot: Perehdytysmenettelyihin sisältyvät taustojen varmistaminen ja politiikan kuittausmekanismit näiden lausekkeiden mukaisesti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personnel Termination) ja PS-5 (Personnel Transfer): Tämä politiikka toimeenpanee käyttöoikeuksien, kulkutunnisteiden ja omaisuuserien jäsennellyn poistamisen tai muuttamisen.

11.3.2 AC-2 (Account Management) ja AC-6 (Least Privilege): Menettelyt varmistavat, että käyttöoikeudet vastaavat roolia ja ne perutaan viipymättä, kun niitä ei enää tarvita.

11.3.3 IA-4 (Identifier Management) ja IA-5 (Authenticator Management): Tukee tunnistetietojen turvallista hallintaa henkilöstömuutosten aikana ja niiden jälkeen.

11.3.4 CM-5 (Access Restrictions for Change): Estää luvattomat työsuhteen päättymisen jälkeiset muutokset peruuttamalla korotetut käyttöoikeudet.

11.3.5 AU-2 ja AU-6: Käyttöoikeustapahtumien lokitusta ja jäljitettävyyttä vahvistetaan IAM-integraation ja audit trailin avulla.

11.4 EU:n GDPR (2016/679):

11.4.1 Artikla 5(1)(f): Suojaa henkilötietoja luvattomalta pääsyltä, mitä tämä politiikka toteuttaa peruuttamalla käyttäjäkäyttöoikeudet poistumisprosessin aikana.

11.4.2 Artikla 32: Edellyttää asianmukaisia teknisiä ja organisatorisia hallintakeinoja henkilötietojen suojaamiseksi työsuhteen elinkaaren aikana.

11.4.3 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Varmistaa, että perehdytys ja työsuhteen päättäminen sisältävät tietojen minimoinnin, säilytyksen ja lainmukaiset käyttöoikeuksien hallintatoimet.

11.4.4 Johdanto-osan kappale 39: Korostaa käyttöoikeuksien rajaamista ja luottamuksellisuutta, joita tämän politiikan rakenne tukee.

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

11.5.1 Artikla 21(2)(b, c, d): Edellyttää henkilöstöön ja toimintaan liittyviä tietoturvatoimenpiteitä pääsynhallinnan, sisäpiiriuhkien torjunnan ja elinkaariprosessien osalta, jotka kaikki sisältyvät tähän politiikkaan.

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

11.6.1 Artikla 5 – Hallinnointi ja sisäinen valvonta: Tämä politiikka tukee henkilöriskeihin ja käyttöoikeuksien hallintaan liittyvää sisäistä ICT-hallinnointia.

11.6.2 Artikla 8 – ICT-riskienhallinta: Soveltaa hallintakeinot henkilöstösiirtymiin, jotka voivat altistaa kriittisiä omaisuuseriä tai säänneltyjä toimintaympäristöjä.

11.6.3 Artikla 9 – Poikkeamien luokittelu ja hallinta: Varmistaa, että työsuhteen päättämiseen liittyvät tietoturvaloukkaukset ovat ilmoitettavia ja että niitä lievennetään asianmukaisella käytöstäpoistolla ja omaisuuden käsittelyllä.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Määrittää perehdytykseen ja työsuhteen päättämiseen liittyvät roolit, vastuut ja elinkaaritoimet hallinnointitavoitteiden mukaisesti.

11.7.2 BAI08 – Knowledge Management: Vahvistaa menettelyjen dokumentointia, tiedon säilyttämistä ja hallintakeinojen siirtoa työsuhteen päättyessä.

11.7.3 DSS05 – Managed Security Services: Toimeenpanee käyttäjien deaktivoinnin, omaisuuden hallinnan ja vastuun osoitettavuuden roolisiirtymien aikana.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Varmistaa, että perehdytyksen ja poistumisprosessin hallintakeinot arvioidaan sisäisissä ja ulkoisissa auditoinneissa.