					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P04					Asiakirjan nimi: **Pääsynhallintapolitiikka**							
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**

Sovitettu soveltuvin osin standardeihin ja säädöksiin

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 5.15, 5.17, 5.18	Loogisen ja fyysisen pääsyn hallinta
ISO/IEC 27002:2022	Kontrollit 8.2, 8.3	Roolipohjainen pääsynhallinta ja identiteetinhallinta
NIST SP 800-53 Rev.5	AC-1–AC-20, IA-1–IA-8	Tilien ja käyttöoikeuksien hallinta, identiteetin todentaminen
EU:n GDPR	Artiklat 5(1)(f), 32(1)(b); johdanto-osan kappale 39	Tietosuoja ja minimointi
EU:n NIS2-direktiivi	Artikla 21(2)(c–e)	Pääsynhallinta, käyttäjän todentaminen ja omaisuuden suojaus
EU:n DORA-asetus	Artiklat 6, 9(2)	ICT- ja käyttäjäpääsy sekä vahvat kontrollit ja kolmannet osapuolet
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Perehdytys, operatiivinen toiminta, seuranta, vaatimustenmukaisuus

1. Tarkoitus

1.1 Tämä politiikka määrittää pakolliset periaatteet, vastuut ja kontrollivaatimukset tietojärjestelmien, sovellusten, fyysisten tilojen ja tietovarojen pääsynhallinnalle koko organisaatiossa.

1.2 Se varmistaa, että pääsy myönnetään liiketoiminnan tarpeen, työtehtävän ja riskitason perusteella sekä että vähimmän oikeuden, tarpeellisuusperiaatteen ja tehtävien eriyttämisen periaatteita noudatetaan.

1.3 Tämä politiikka tukee ISO/IEC 27001:2022 -standardin kohdan 5.15 ja siihen liittyvien loogista ja fyysistä pääsyä, käyttäjän todentamista sekä pääsyn elinkaaren hallintaa koskevien kontrollien toteutusta.

1.4 Tämä politiikka tukee digitaalisten ja fyysisten resurssien suojaamista luvattomalta käytöltä, väärinkäytöltä ja vaarantumiselta.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia ISMS:n soveltamisalaan kuuluvia käyttäjiä, järjestelmiä ja tiloja, mukaan lukien:

2.1.1 työntekijät, alihankkijat, toimittajat ja tilapäinen henkilöstö

2.1.2 paikallisesti ylläpidetty infrastruktuuri, pilvipalveluissa toimivat järjestelmät ja hybridiympäristöt

2.1.3 kaikki organisaation omaisuuserät — laitteistot, ohjelmistot, tiedot ja suojatut fyysiset alueet

2.1.4 looginen pääsy (esim. järjestelmät, verkot, sovellukset, API-rajapinnat) ja fyysinen pääsy (esim. rakennukset, konesalit)

2.2 Politiikka ohjaa pääsynhallintaa koko identiteetin ja resurssien käytön elinkaaren ajan perehdytyksestä ja käyttöoikeuksien myöntämisestä roolimuutoksiin ja käyttöoikeuksien päättämiseen.

2.3 Politiikka kattaa myös omien laitteiden käytön (BYOD) ja etäkäytön sekä varmistaa, että kontrollit ovat yhdenmukaiset eri sijainneissa ja laitteiden omistusmalleissa.

3. Tavoitteet

3.1 Toteuttaa turvalliset, roolipohjaiset pääsynhallintakontrollit, jotka tukevat toiminnallista eheyttä ja vaatimustenmukaisuutta.

3.2 Varmistaa, että käyttöoikeudet hyväksytään asianmukaisesti, niitä valvotaan ja ne poistetaan oikea-aikaisesti.

3.3 Estää luvaton pääsy, käyttöoikeuksien laajentaminen sekä vanhentuneiden käyttöoikeuksien jääminen voimaan.

3.4 Tukea Zero Trust -periaatteita siten, että pääsy estetään oletusarvoisesti, ellei sitä ole nimenomaisesti hyväksytty ja perusteltu.

3.5 Tuottaa auditoijille ja sidosryhmille todentavaa aineistoa automatisoitujen, näyttöön perustuvien käyttöoikeuskatselmusten ja politiikan soveltamisen kautta.

3.6 Sisällyttää pääsynhallinta liiketoimintaprosesseihin, henkilöstön elinkaaritapahtumiin ja teknisiin arkkitehtuureihin.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy pääsynhallintapolitiikan ja varmistaa sen toimeenpanoon tarvittavat resurssit ja henkilöstön.

4.1.2 Käsittelee pääsynhallinnan riskejä johdon katselmuksissa ja osoittaa vastuut strategisella tasolla.

4.2 CISO / ISMS-päällikkö

4.2.1 Vastaa pääsynhallinnan viitekehyksestä ja varmistaa sen yhdenmukaisuuden ISO/IEC 27001 -standardin ja siihen liittyvien standardien kanssa.

4.2.2 Koordinoi politiikan toimeenpanoa, kontrollien testausta ja pääsynhallinnan mittareiden raportointia.

4.2.3 Valvoo riskiperusteista pääsyn mallintamista ja seuraa järjestelmätason kontrollipuutteita.

[... 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 vuosittain, tai

9.1.1.2 merkittävän IT-infrastruktuurin, sääntelyvaatimusten tai riskitason muutoksen jälkeen

9.1.1.3 sellaisten poikkeamien jälkeen, jotka paljastavat heikkouksia pääsynhallintakontrolleissa

9.1.1.4 kun todentamisteknologioissa tai identiteettialustoissa tapahtuu merkittäviä muutoksia

9.2 Katselmointivastuu ja prosessi

9.2.1 CISO tai nimetty ISMS-vastuuhenkilö hallinnoi katselmointisykliä ja ottaa huomioon seuraavat:

9.2.1.1 sisäisen tarkastuksen havainnot

9.2.1.2 käyttöoikeuskatselmusten tulokset ja mittarit

9.2.1.3 lainsäädännön ja sääntelyn päivitykset

9.2.1.4 teknologiaympäristön muutokset

9.2.2 Ylimmän johdon on hyväksyttävä kaikki muutokset, ja niistä on viestittävä kaikille sidosryhmille.

9.2.3 Vaikutuksen kohteena olevilta käyttäjiltä voidaan edellyttää politiikan uudelleenhyväksyntää olennaisten päivitysten jälkeen.

9.3 Versionhallinta ja dokumentointi

9.3.1 Pääversio on säilytettävä ISMS:n dokumenttirekisterissä seuraavin metatiedoin:

9.3.1.1 versionumero ja muutosloki

9.3.1.2 voimaantulopäivä ja seuraava katselmointipäivä

9.3.1.3 omistaja ja hyväksyvä taho

9.3.1.4 jakelu- ja hyväksymiskirjaukset

9.3.2 Korvatut versiot on arkistoitava ja pidettävä saatavilla vähintään 3 vuoden ajan.

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa on tulkittava yhdessä seuraavien kanssa, ja se on toiminnallisesti riippuvainen niistä:

10.1.1 P01 – Tietoturvapolitiikka: määrittää organisaation tietoturvasitoumuksen ja korkean tason odotukset pääsynhallinnalle.

10.1.2 P03 – Hyväksyttävän käytön politiikka: määrittää pääsyyn liittyvät käyttäytymisvaatimukset ja käyttäjien vastuun järjestelmien asianmukaisesta käytöstä.

10.1.3 P05 – Muutoksenhallintapolitiikka: ohjaa, miten pääsyasetuksiin, rooleihin tai ryhmärakenteisiin tehtävät muutokset toteutetaan ja testataan turvallisesti.

10.1.4 P07 – Perehdytys- ja päättämispolitiikka: ohjaa käyttöoikeuksien myöntämistä ja poistamista käyttäjän elinkaaritapahtumien mukaisesti.

10.1.5 P11 – Käyttäjätilien ja käyttöoikeuksien hallintapolitiikka: toimeenpanee käytännön tason kontrollit ja täydentää tätä politiikkaa teknisillä pääsynhallinnan ohjeilla.

10.2 Yhdessä nämä politiikat muodostavat yhtenäisen ja toimeenpantavan pääsynhallinnan viitekehyksen liiketoimintayksiköissä ja teknologia-alueilla.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:2022:

11.1.1 Kohta 5.15 – Pääsynhallinta: tämä politiikka täyttää vaatimuksen tiedon ja muiden siihen liittyvien omaisuuserien pääsyn hallinnasta liiketoiminnan ja tietoturvan vaatimusten perusteella.

11.1.2 Kohta 5.17 – Identiteetinhallinta ja kohta 5.18 – Todentamistiedot: nämä toteutetaan identiteetin provisioinnin, todentamismekanismien ja käyttöoikeuksien määritysten kautta.

11.1.3 Liitteen A kontrollit 8.2 (Pääsynhallinta) ja 8.3 (Identiteetinhallinta): ne muodostavat tämän politiikan kontrollitavoitteiden perustan, mukaan lukien roolipohjainen pääsy, käyttäjän elinkaaren integrointi ja etuoikeutetun pääsyn suojaus.

11.2 NIST SP 800-53 Rev.5:

11.2.1 AC-perhe (AC-1–AC-20): tämä politiikka tukee NISTin pääsynhallintavaatimuksia sekä fyysisille että loogisille järjestelmille, mukaan lukien politiikan määrittely (AC-1), tilinhallinta (AC-2) ja tehtävien eriyttäminen (AC-5).

11.2.2 IA-perhe (IA-1–IA-8): antaa ohjeistusta identiteetin todentamiseen, tunnistetietojen suojaamiseen ja MFA:n käyttöön.

11.2.3 AU-2, AU-12: tämän politiikan mukaiset lokitus- ja auditointivaatimukset tukevat käyttäjävastuullisuutta ja poikkeamien tutkintaa.

11.2.4 PE-2–PE-6: koskevat fyysisen pääsyn rajoituksia, joita tämä politiikka osittain toteuttaa kulkutunnistekontrollien ja rakennusten pääsyoikeuksien avulla.

11.3 EU:n GDPR (2016/679):

11.3.1 Artikla 5(1)(f): henkilötiedot on suojattava luvattomalta pääsyltä. Tämä politiikka varmistaa kyseisen periaatteen teknisen ja menettelyllisen toteutuksen.

11.3.2 Artikla 32(1)(b): edellyttää pääsynhallintakontrollien, pseudonymisoinnin ja salauksen toteuttamista henkilötietojen luvattoman käsittelyn estämiseksi.

11.3.3 Johdanto-osan kappale 39: edellyttää henkilötietoihin kohdistuvan pääsyn minimointia, jota tässä politiikassa toteutetaan vähimmän oikeuden periaatteella ja pääsyn perusteluvaatimuksilla.

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

11.4.1 Artikla 21(2)(c–e): tämä politiikka mahdollistaa tekniset ja organisatoriset toimenpiteet pääsynhallinnan, käyttäjän todentamisen ja omaisuuden suojaamisen osalta keskeisissä ja tärkeissä toimijoissa.

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

11.5.1 Artikla 6: edellyttää ICT-riskienhallintapolitiikkoja, jotka sisältävät nimenomaisesti käyttäjien pääsynhallinnan ja identiteetin elinkaaren kontrollit. Tämä politiikka täyttää kyseisen vaatimuksen rahoitus- ja ICT-palvelualoilla.

11.5.2 Artikla 9(2): tämä politiikka tukee vahvojen pääsynhallintakontrollien soveltamista osana kolmansien osapuolten ja konsernin sisäisten ICT-palvelujen hallintaa.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: toimeenpanee perehdytys- ja poistumiskontrollit pääsynhallinnan tukemiseksi.

11.6.2 BAI03 – Managed Solutions Identification and Build: sisällyttää pääsynhallintavaatimukset järjestelmäsuunnitteluun ja muutoksenhallintaprosesseihin.

11.6.3 DSS01 – Managed Operations ja DSS05 – Managed Security Services: ohjaavat loogisen pääsyn rajoitusten soveltamista ja rikkomusten seurantaa.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: tukee auditointi- ja varmennusmekanismeja pääsynhallinnan tehokkuuden todentamiseksi.