					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P04S					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 standardeihin ja sääntelyvaatimuksiin

Standardi/sääntely	Kohta/artikla	Huomio
ISO/IEC 27001:2022	Kohta 5	
ISO/IEC 27002:2022	Hallintakeinot 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1–AC-5	
EU:n GDPR	Artikla 32	
EU:n NIS2-direktiivi	Artikla 21(2)(b)	
EU:n DORA-asetus	Artikla 9	
COBIT 2019	APO07, DSS01	

1. Tarkoitus

1.1. Tämä politiikka määrittää, miten organisaatio hallinnoi pääsyä järjestelmiin, tietoihin ja tiloihin varmistaakseen, että vain valtuutetut henkilöt voivat käyttää tietoja liiketoiminnallisen tarpeen perusteella.

1.2. Politiikka määrittää selkeät säännöt käyttäjätunnusten myöntämiselle, muuttamiselle, valvonnalle ja poistamiselle luvattoman pääsyn riskin minimoimiseksi sekä sovellettavien lakien ja standardien noudattamisen tukemiseksi.

1.3. Tämä politiikka edellyttää vähimmän oikeuden periaatteen noudattamista siten, että käyttöoikeudet rajataan työtehtävien hoitamisen kannalta välttämättömään minimiin.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkia henkilöitä, jotka käyttävät tai hallinnoivat pääsyä organisaation IT-järjestelmiin, verkkoihin, tietoihin tai tiloihin, mukaan lukien:

2.1.1. Työntekijät

2.1.2. Sopimuskumppanit

2.1.3. Tilapäiset työntekijät

2.1.4. Ulkoiset IT-palveluntarjoajat

2.2. Politiikka kattaa pääsyn seuraaviin:

2.2.1. Organisaation sovellukset, tiedostojakoalueet ja tietokannat

2.2.2. Sähköposti-, VPN- ja etäyhteysjärjestelmät

2.2.3. Liiketoimintakäyttöön tarkoitetut pilvipalvelut

2.2.4. Fyysinen pääsy suojattuihin tiloihin, kuten toimistoihin tai palvelinhuoneisiin

2.3. Tätä politiikkaa sovelletaan kaikkiin laitteisiin (organisaation toimittamiin tai hyväksyttyihin BYOD-laitteisiin), alustoihin ja sijainteihin.

3. Tavoitteet

3.1. Varmistaa, että käyttöoikeuksia myönnetään vain muodollisen hyväksynnän jälkeen roolin ja liiketoiminnallisen tarpeen mukaisesti.

3.2. Estää luvaton tai tarpeettoman laaja pääsy arkaluonteisiin tietoihin, järjestelmiin tai infrastruktuuriin.

3.3. Määrittää selkeät menettelyt käyttäjien käyttöoikeuksien myöntämiselle, muuttamiselle ja poistamiselle.

3.4. Edellyttää säännöllisiä käyttöoikeuskatselmointeja sekä automaattista tai manuaalista lokitusta auditointien tueksi.

3.5. Tukea käyttöoikeusrajoitusten teknistä toteutusta konfiguroinnin ja valvonnan avulla.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. Hyväksyy tämän politiikan ja varmistaa, että tehokkaiden pääsynhallintakeinojen toteuttamiseen on käytettävissä riittävät resurssit.

4.1.2. Hyväksyy poikkeukset ja katselmoi vuosittaiset käyttöoikeusauditoinnit.

4.2. IT-päällikkö / ulkoinen IT-palveluntarjoaja

4.2.1. Vastaa käyttäjätilien perustamisesta, muuttamisesta ja poistamisesta.

4.2.2. Ylläpitää pääsynhallintarekisteriä, johon kirjataan kaikki toimenpiteet (perustamiset, muutokset, poistot).

4.2.3. Toteuttaa roolipohjaisen käyttöoikeuksien hallinnan (RBAC) ja ottaa käyttöön vahvan tunnistautumisen (esim. MFA).

4.2.4. Tarkastaa käyttöoikeuslokeja epäilyttävän toiminnan havaitsemiseksi ja raportoi havainnot toimitusjohtajalle.

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Politiikan vuosittainen katselmointi

9.1.1. IT-päällikön tulee katselmoida tämä politiikka vuosittain. Oikeudellisessa, teknisessä tai organisatorisessa toimintaympäristössä tapahtuvien muutosten tulee käynnistää välitön päivitys.

9.2. Katselmoinnin käynnistävät tekijät

9.2.1. Politiikka tulee katselmoida myös, jos jokin seuraavista toteutuu:

9.2.2. Merkittävät järjestelmämuutokset tai siirtymät pilvipalveluihin

9.2.3. Muutokset rooleissa tai organisaatiorakenteessa

9.2.4. Tietoturvapoikkeama, johon liittyy luvatonta pääsyä

9.2.5. Sääntelymuutokset (esim. EU:n GDPR:n, EU:n NIS2-direktiivin tai EU:n DORA-asetuksen päivitykset)

9.3. Muutosten dokumentointi ja viestintä

9.3.1. Muutokset tulee kirjata versiohistoriaan, hyväksyttää toimitusjohtajalla ja viestiä kaikille henkilöille, joita muutos koskee.

9.4. Saatavuus ja koulutus

9.4.1. Tämä politiikka tulee saattaa koko henkilöstön saataville, ja asiaankuuluva koulutus tulee järjestää osana perehdytystä ja sen jälkeen vuosittain.

10. Liittyvät politiikat ja yhteydet

10.1. Tätä politiikkaa tulee soveltaa yhdessä seuraavien pk-yrityksille tarkoitettujen politiikkojen kanssa turvallisten pääsynhallintakäytäntöjen kattavan toteutuksen varmistamiseksi:

10.1.1. P3S – Hyväksyttävän käytön politiikka: Varmistaa, että käyttäjät ymmärtävät hyväksyttävän toiminnan myönnettyjen käyttöoikeuksien puitteissa.

10.1.2. P5S – Muutoksenhallintapolitiikka: Varmistaa, että käyttöoikeudet vastaavat hyväksyttyjä järjestelmämuutoksia.

10.1.3. P7S – Perehdytys- ja päättämispolitiikka: Määrittää käyttäjien käyttöoikeuksien myöntämisen ja poistamisen käynnistävät tapahtumat.

10.1.4. P17S – Tietosuoja- ja yksityisyyspolitiikka: Varmistaa, että pääsynhallinta vastaa henkilötietojen suojaa koskevia vaatimuksia.

10.1.5. P30S – Tietoturvapoikkeamien hallintapolitiikka: Määrittää, miten käyttöoikeuksiin liittyviä poikkeamia (esim. väärinkäyttö tai tietomurrot) hallitaan ja tutkitaan.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 5.15 – Edellyttää muodollisia pääsynhallintapolitiikkoja ja -prosesseja.

11.2. ISO/IEC 27002

11.2.1. Hallintakeinot 5.15–5.17 – Antavat yksityiskohtaisia ohjeita roolipohjaisesta käyttöoikeuksien hallinnasta, käyttäjän elinkaaren hallinnasta ja etuoikeutettujen käyttöoikeuksien hallinnasta.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1–AC-5 – Edellyttävät jäsenneltyjä käyttöoikeuksien hallinnan politiikkoja, mukaan lukien tilien valtuuttaminen, katselmointi ja seuranta.

11.4. EU:n GDPR

11.4.1. Artikla 32 – Edellyttää teknisiä ja organisatorisia hallintakeinoja (kuten käyttöoikeuksien hallintaa) tietoturvan ja luottamuksellisuuden varmistamiseksi.

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(b) – Edellyttää operatiivista pääsynhallintaa ja identiteetinhallintajärjestelmiä luvattoman järjestelmäpääsyn estämiseksi.

11.6. EU:n DORA-asetus

11.6.1. Artikla 9 – Korostaa ICT-riskien turvallista hallintaa, mukaan lukien vahva pääsynhallinta finanssialan toimijoille.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: Edellyttää määriteltyjä ja toimeenpantuja pääsynhallinnan vastuita.

11.7.2. DSS01 – Manage Operations: Sisältää menettelyt loogisen pääsyn hallintaan ja turvallisten käyttöympäristöjen ylläpitämiseen.