					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P11S					Asiakirjan nimi: **Käyttäjätilien ja etuoikeuksien hallintapolitiikka**							
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/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lausekkeet 5.3, 8	Roolit, vastuut sekä operatiivinen suunnittelu ja kontrollit käyttäjien käyttöoikeuksien hallintaa varten
ISO/IEC 27002:2022	Kontrolli 8	Kontrollit etuoikeuksien myöntämiseen, katselmointiin ja poistamiseen
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Tilien luominen, seuranta, vähimmän oikeuden periaate ja tehtävien eriyttäminen
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Käyttäjien käyttöoikeuksien hallinta keskeisille ja tärkeille toimijoille
EU:n DORA-asetus	Artikla 9(2)(b)	Etuoikeutetun pääsyn hallinta finanssialan toimijoissa
COBIT 2019	DSS05.03, DSS05.04	Käyttöoikeuksien myöntäminen, poistaminen ja säännöllinen katselmointi
EU:n GDPR	Artikla 32	Asianmukaiset pääsynhallintatoimet henkilötietojen suojaamiseksi

1. Tarkoitus

1.1 Tällä politiikalla määritetään käyttäjätilien ja käyttöoikeuksien hallintaa koskevat säännöt turvallisella, yhdenmukaisella ja jäljitettävällä tavalla. Politiikka varmistaa, että vain valtuutetuilla käyttäjillä on pääsy järjestelmiin ja tietoihin ja että käyttöoikeudet vastaavat käyttäjän roolia ja vastuita.

1.2 Tehokas käyttäjätilien ja etuoikeuksien hallinta on olennaista luvattoman pääsyn estämiseksi, sisäisten uhkien minimoimiseksi sekä ISO/IEC 27001:n, EU:n GDPR:n ja muiden sääntelyvaatimusten noudattamisen varmistamiseksi.

1.3 Tämän politiikan avulla organisaatio määrittää käyttäjätilien käytön omistajuuden ja vastuut, seuraa ja auditoi käyttöoikeuksien korotuksia sekä estää tai peruuttaa käyttöoikeudet turvallisesti silloin, kun niitä ei enää tarvita.

1.4 Politiikka suojaa myös liiketoimintaa operatiivisilta virheiltä ja väärinkäytöksiltä, joita liialliset tai valvomattomat käyttöoikeudet voivat aiheuttaa, ja auttaa vähentämään tahattomien tietovuotojen, etuoikeuksien väärinkäytön tai sääntelyvaatimusten noudattamatta jättämisen riskiä.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 kaikkiin työntekijöihin, harjoittelijoihin, sopimuskumppaneihin ja kolmansien osapuolten käyttäjiin, joilla on pääsy organisaation IT-järjestelmiin

2.1.2 kaikkiin järjestelmiin, laitteisiin, palveluihin ja alustoihin, joita hallinnoidaan organisaation toimesta tai sen puolesta, mukaan lukien pilvialustat, paikallinen infrastruktuuri ja kolmansien osapuolten työkalut

2.2 Politiikka kattaa kaikentyyppiset käyttäjätilit, mukaan lukien:

2.2.1 nimetyt käyttäjätilit (esim. sähköpostitilit, järjestelmäkirjautumiset)

2.2.2 ylläpitäjätilit ja järjestelmätason tilit

2.2.3 tilapäiset, vieras- tai kolmansien osapuolten tunnistetiedot

2.2.4 sovellusten tai automaatiojärjestelmien käyttämät palvelutilit

2.3 Politiikkaa sovelletaan koko käyttäjätilin elinkaaren ajan luonnista ja hyväksynnästä muutoksiin, seurantaan ja käytöstä poistamiseen. Tämä sisältää käyttöoikeuksien myöntämisen perehdytyksen aikana, käyttöoikeuskatselmoinnit roolimuutosten yhteydessä sekä käyttöoikeuksien poistamisen palvelussuhteen päättämisen yhteydessä.

3. Tavoitteet

3.1 Määrittää kaikille järjestelmien käyttäjille yksilölliset ja jäljitettävät käyttäjäidentiteetit, jotta vastuut voidaan osoittaa eikä jaettuihin tunnuksiin tarvitse tukeutua.

3.2 Toteuttaa vähimmän oikeuden periaate siten, että käyttäjille myönnetään vain heidän tehtäviensä hoitamiseen välttämättömät vähimmäiskäyttöoikeudet.

3.3 Estää luvaton pääsy arkaluonteisiin järjestelmiin tai tietoihin selkeästi dokumentoitujen hyväksyntä- ja katselmointimenettelyjen avulla.

3.4 Varmistaa käyttäjätilien oikea-aikainen käytöstä poisto, kun niitä ei enää tarvita, esimerkiksi työsuhteen päättyessä, sopimuksen päättyessä tai roolin muuttuessa.

3.5 Ylläpitää turvallista ympäristöä ja auditointivalmiutta dokumentoimalla kaikki käyttäjätileihin liittyvät muutokset, hyväksynnät ja säännölliset katselmoinnit.

3.6 Varmistaa, että käyttöoikeuksien korotuksia hallitaan tiukasti, ne hyväksytään riippumattomasti ja kirjataan lokiin sekä että korotetut käyttöoikeudet peruutetaan viipymättä, kun niitä ei enää tarvita.

4. Roolit ja vastuut

4.1 Toimitusjohtaja

4.1.1 Vastaa tämän politiikan kokonaisvaltaisesta soveltamisesta.

4.1.2 Varmistaa, että käyttäjätilien hallintakäytännöt ovat ISO/IEC 27001 -sertifiointivaatimusten ja sovellettavien lakisääteisten velvoitteiden (esim. EU:n GDPR) mukaisia.

4.1.3 Hänelle on ilmoitettava välittömästi kaikesta luvattomasta pääsystä, tietoturvapoikkeamasta tai politiikan rikkomuksesta, joka liittyy käyttäjätileihin.

4.1.4 Valvoo politiikan katselmointeja, auditointeja ja soveltamistoimenpiteitä.

4.2 IT-vastaava tai ulkoinen IT-palveluntarjoaja

4.2.1 Vastaa käyttäjätili- ja etuoikeushallinnan kontrollien teknisestä toteutuksesta organisaation käyttämissä järjestelmissä.

4.2.2 Saa luoda, muuttaa ja poistaa käyttäjätilejä käytöstä vain dokumentoitujen hyväksyntöjen perusteella.

4.2.3 Hänen on toteutettava salasanojen monimutkaisuusvaatimukset, näytön aikakatkaisu, monivaiheinen todennus, jos se on käytettävissä, sekä järjestelmälokitus.

4.2.4 Hänen on ylläpidettävä turvallisesti kaikkia käyttöoikeushyväksyntöjä, käyttäjätilien omistajuutta, käyttöoikeuksien korotuksia ja käyttöoikeuksien peruutuksia koskevia tallenteita.

4.2.5 Hänen on seurattava luvattomia tai orpoja tilejä ja raportoitava poikkeamat toimitusjohtajalle.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Toimitusjohtajan ja IT-vastaavan on katselmoitava tämä politiikka vähintään kerran vuodessa varmistaakseen yhdenmukaisuuden seuraavien kanssa:

9.1.1 voimassa olevat ISO/IEC 27001:2022 -kontrollit ja ohjeistus

9.1.2 sääntelymuutokset (esim. EU:n GDPR, DORA-asetus, EU:n NIS2-direktiivi)

9.1.3 muutokset järjestelmissä, palveluissa tai liiketoimintarakenteessa

9.2 Katselmointi on tehtävä myös seuraavien jälkeen:

9.2.1 merkittävät tietoturvapoikkeamat tai auditointihavainnot

9.2.2 merkittävät muutokset IT-järjestelmissä tai käyttäjätiliarkkitehtuurissa

9.2.3 uusien alustojen käyttöönotto, joka edellyttää pääsynhallinnan integrointia

9.3 Kaikki muutokset on hyväksyttävä toimitusjohtajan toimesta, ja niistä on viestittävä selkeästi vaikutuksen kohteena olevalle henkilöstölle.

10. Liittyvät politiikat ja yhteydet

10.1 P2S – Hallinnointirooleja ja vastuita koskeva politiikka: määrittää vastuut ja päätöksentekovaltuudet käyttöoikeuksien hyväksynnöille ja valvonnalle.

10.2 P4S – Pääsynhallintapolitiikka: ohjaa järjestelmätasoista pääsynhallinnan toteutusta ja todennusmenetelmiä.

10.3 P7S – Perehdytys- ja työsuhteen päättämispolitiikka: varmistaa, että käyttäjätilien luominen ja poistaminen sisältyvät henkilöstöhallinnon hallitsemiin henkilöstömuutoksiin.

10.4 P8S – Tietoturvatietoisuus- ja koulutuspolitiikka: kouluttaa käyttäjiä turvallisiin käyttäjätilikäytäntöihin ja käyttöä koskeviin odotuksiin.

10.5 P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää toimenpiteet tilanteissa, joissa käyttäjätilien väärinkäyttö johtaa tietomurtoon tai luvattomaan tietojen luovutukseen.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 5.3: edellyttää, että tietoturvallisuuden roolit ja vastuut määritetään selkeästi ja niitä noudatetaan.

11.1.2 Lauseke 8.1: operatiivisen suunnittelun ja kontrollien on sisällettävä käyttäjien käyttöoikeuksien hallinta.

11.2 ISO/IEC 27002

11.2.1 Kontrolli 8.2: kuvaa tekniset ja menettelylliset kontrollit etuoikeuksien myöntämiseen, katselmointiin ja poistamiseen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: edellyttää käyttäjätilien luomista, seurantaa ja käyttöoikeuksien perumista määriteltyjen roolien ja prosessien perusteella.

11.3.2 AC-5: käsittelee tehtävien eriyttämistä eturistiriitojen tai etuoikeuksien väärinkäytön estämiseksi.

11.3.3 AC-6: edellyttää vähimmän oikeuden periaatteen soveltamista kaikkiin käyttöoikeuksiin.

11.4 EU:n GDPR

11.4.1 Artikla 32: edellyttää asianmukaisia pääsynhallintatoimia henkilötietojen suojaamiseksi luvattomalta pääsyltä tai muuttamiselta.

11.5 EU:n NIS2-direktiivi

11.5.1 Artikla 21(2)(d): edellyttää käyttäjien käyttöoikeuksien hallintaa osana keskeisiä tietoturvakontrolleja keskeisille ja tärkeille toimijoille.

11.6 EU:n DORA-asetus

11.6.1 Artikla 9(2)(b): edellyttää finanssialan toimijoilta pääsynhallintatoimia, joilla rajoitetaan ja valvotaan etuoikeutettuja oikeuksia.

11.7 COBIT 2019

11.7.1 DSS05.03: määrittää käyttöoikeuksien myöntämisen ja poistamisen osaksi IT-hallintoa.

11.7.2 DSS05.04: edellyttää käyttäjien käyttöoikeuksien jatkuvaa katselmointia ja yhdenmukaistamista organisaation roolien kanssa.