					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P21S					Asiakirjan nimi: **Verkkoturvallisuuspolitiikka**							
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	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 8	-
ISO/IEC 27002:2022	Kontrolli 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
EU:n GDPR	Artikla 32	-
EU:n NIS2-direktiivi	Artiklat 21(2)(d), (e)	-
EU:n DORA-asetus	Artiklat 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Tarkoitus

1.1. Tämän politiikan tarkoituksena on varmistaa, että kaikki sisäiset ja ulkoiset verkkoyhteydet suojataan luvattomalta käytöltä, peukaloinnilta, salakuuntelulta ja väärinkäytöltä selkeästi määritellyillä tietoturvakontrolleilla.

1.2. Tämä politiikka määrittää vaatimukset verkkoinfrastruktuurin turvalliselle suunnittelulle, käytölle ja hallinnalle, mukaan lukien reitittimet, langattomat tukiasemat, etäyhteydet ja segmentoitu verkkoarkkitehtuuri.

1.3. Tavoitteena on minimoida altistuminen internetpohjaisille uhille, varmistaa sisäisissä ja ulkoisissa verkoissa siirrettävien tietojen luottamuksellisuus sekä ylläpitää kriittisten palvelujen saatavuutta.

1.4. Tämä politiikka tukee ISO/IEC 27001:2022 -sertifiointia ja edistää GDPR:n, NIS2:n ja DORA:n mukaisten lakisääteisten ja sääntelyyn liittyvien velvoitteiden täyttämistä sekä tarjoaa teknistä varmuutta asiakkaille ja auditoijille.

2. Soveltamisala

2.1. Tätä politiikkaa sovelletaan kaikkiin organisaation IT-verkon osa-alueisiin, mukaan lukien:

2.1.1. Toimipaikkojen kiinteä ja langaton verkkoinfrastruktuuri

2.1.2. Reitittimet, kytkimet, tukiasemat, palomuurit ja yhdyskäytävät

2.1.3. Etäyhteydet, mukaan lukien VPN-yhteydet, RDP ja pilvitunnelit

2.1.4. Pilvipohjaiset sovellukset, joita käytetään sisäisistä tai ulkoisista verkoista

2.1.5. Laitteet, jotka työntekijät, sopimuskumppanit tai vierailijat liittävät verkkoon

2.2. Tämä politiikka koskee sekä fyysisiä että loogisia verkkosegmenttejä, mukaan lukien vierasverkot, IoT-laitteet ja taustajärjestelmät.

2.3. Politiikka koskee kaikkea henkilöstöä, jolla on pääsy organisaation verkkoon, mukaan lukien:

2.3.1. Organisaation työntekijät

2.3.2. Etä- ja hybridityötä tekevä henkilöstö

2.3.3. Ulkoiset toimittajat, konsultit ja palveluntarjoajat

2.3.4. Vierailijat, joille on myönnetty tilapäinen Wi-Fi-yhteys

3. Tavoitteet

3.1. Varmistaa, että organisaation verkko on suojattu luvattomalta käytöltä ja ulkoisilta kyberuhilta

3.2. Varmistaa asianmukainen segmentointi luotettujen ja epäluotettujen verkkojen välillä (esim. vieras-Wi-Fi, toimittajien pääsy)

3.3. Mahdollistaa turvalliset etäyhteydet vaarantamatta sisäisiä järjestelmiä

3.4. Estää haittaohjelmien leviäminen ja tietojen luvaton siirto verkkokanavien kautta

3.5. Varmistaa verkkotoiminnan seuranta, hälytykset ja auditointikelpoinen lokitus poikkeamien havaitsemisen ja vaatimustenmukaisuuden tueksi

3.6. Varmistaa, että vain hyväksytyt ja suojatut laitteet voivat liittyä sisäisiin verkkoihin

3.7. Täyttää ISO 27001:n, GDPR:n ja niihin liittyvien kyberturvallisuusviitekehysten velvoitteet

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. Omistaa tämän politiikan ja varmistaa, että turvalliseen verkkosuunnitteluun ja verkonhallintaan osoitetaan asianmukaiset resurssit

4.1.2. Katselmoi verkkoturvallisuuden kontrollipoikkeukset ja hyväksyy toimittajien verkkopääsyä koskevat sopimukset

4.1.3. Katselmoi verkkoturvallisuuden heikkouksiin liittyvät poikkeamat ja auditointihavainnot

4.2. IT-palveluntarjoaja / sisäinen IT-vastaava

4.2.1. Toteuttaa, konfiguroi ja ylläpitää kaikki palomuurit, reitittimet, kytkimet ja langattomat ohjaimet

4.2.2. Hallinnoi segmentointia sisäisten, vieras- ja ulkoisten verkkojen välillä

4.2.3. Seuraa lokeja ja hälytyksiä luvattomien pääsy-yritysten ja verkkopoikkeamien havaitsemiseksi

4.2.4. Varmistaa, että laiteohjelmisto- ja konfiguraatiopäivitykset toteutetaan turvallisesti ja oikea-aikaisesti

[... 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. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa yhdessä IT-palveluntarjoajan ja tietosuojakoordinaattorin kanssa.

9.2. Katselmoinnin käynnistävät tapahtumat

9.2.1. Politiikan katselmointi on käynnistettävä myös seuraavissa tilanteissa:

9.2.1.1. Merkittävät muutokset verkkoarkkitehtuurissa (esim. uudet VPN- tai palomuurijärjestelmät)

9.2.1.2. Verkkoon liittyvä poikkeama (esim. tunkeutuminen, kiristyshaittaohjelman leviäminen tai tietojen luvaton siirto)

9.2.1.3. Verkon suojaamiseen vaikuttavat lakien, sääntelyn tai viitekehysten muutokset

9.2.1.4. Uudet toimittaja-alustat, jotka edellyttävät vaihtoehtoisia pääsytapoja tai protokollia

9.3. Versionhallinta ja dokumentointi

9.3.1. Politiikan muutokset on kirjattava versionumerolla, päivämäärällä ja muutosten yhteenvedolla

9.3.2. Aiemmat versiot on arkistoitava vähintään 3 vuoden ajaksi

9.3.3. Päivityksistä on tiedotettava niille työntekijöille, joita ne koskevat, ja merkittävien toimintatapamuutosten yhteydessä on edellytettävä hyväksyntää

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka on toteutettava yhdessä seuraavien pk-yrityksen tietoturvapolitiikkojen kanssa:

10.1.1. P9S – Etätyöpolitiikka: määrittää turvalliset etäkäyttötavat, VPN-vaatimukset ja päätelaitteiden suojauksen muualla kuin toimipaikassa työskenteleville käyttäjille.

10.1.2. P12S – Omaisuudenhallintapolitiikka: varmistaa, että kaikki verkkoon liitetyt järjestelmät tunnistetaan, luokitellaan ja niitä valvotaan ajantasaisen tietoturvatilan perusteella.

10.1.3. P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: varmistaa, että verkon segmentointi, pääsynhallinta ja lokitus tukevat GDPR:n mukaisia tietosuojan ja yksityisyydensuojan periaatteita.

10.1.4. P22S – Lokitus- ja valvontapolitiikka: määrittää vaatimukset verkkolaitteiden, etäyhteyksien ja langattomien ohjainten lokien keräämiselle ja katselmoinnille.

10.1.5. P30S – Tietoturvapoikkeamien hallintapolitiikka: määrittää vaaditut toimenpiteet tilanteissa, joissa sisäisten verkkojen kautta tapahtuu tietoturvaloukkauksia, luvattomia pääsy-yrityksiä tai haittaohjelmien leviämistä.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 8.1 – Edellyttää kontrollien toteuttamista turvallisen ja häiriönsietokykyisen toiminnan varmistamiseksi, mukaan lukien verkot.

11.2. ISO/IEC 27002

11.2.1. Kontrolli 8.20 – Antaa teknisiä ja menettelyllisiä ohjeita verkkoon pääsyn, segmentoinnin ja seurannan suojaamiseen.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Edellyttää tiedonkulun hallintaa verkoissa ja järjestelmien välillä.

11.3.2. SC-7 – Edellyttää rajasuojauksia, turvallista reititystä ja verkon segmentointia luvattoman pääsyn riskin vähentämiseksi.

11.4. EU:n GDPR

11.4.1. Artikla 32 – Edellyttää asianmukaisia teknisiä ja organisatorisia toimenpiteitä henkilötietoja käsittelevien verkotettujen järjestelmien ja palvelujen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi.

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(d) – Edellyttää riskiperusteisia teknisiä toimenpiteitä, mukaan lukien verkkoturvallisuus ja pääsynhallinta.

11.5.2. Artikla 21(2)(e) – Edellyttää järjestelmien segmentointia ja eristämistä kyberpoikkeamien leviämisen estämiseksi.

11.6. EU:n DORA-asetus

11.6.1. Artikla 9 – Edellyttää organisaatioilta ICT-riskienhallinnan kontrollien toteuttamista, mukaan lukien turvallisia verkkoja ja viestintää koskevat kontrollit.

11.6.2. Artikla 10 – Edellyttää, että digitaalisen häiriönsietokyvyn strategiat kattavat verkkoinfrastruktuurin ja etäyhteyksien suojauksen.

11.7. COBIT 2019

11.7.1. DSS05.02 – Edellyttää IT-infrastruktuurin ja verkkoympäristöjen tehokasta suojaamista sisäisiä ja ulkoisia uhkia vastaan.

11.7.2. APO13.01 – Edellyttää riskienhallintastrategioita, joihin sisältyvät verkon segmentointi ja seuranta osana uhkien lieventämistä.