					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P21					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	Ei sovelleta
ISO/IEC 27002:2022	Kontrollit 8.20–8.22	Ei sovelleta
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	Ei sovelleta
EU:n GDPR	Artikla 32	Ei sovelleta
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Ei sovelleta
EU:n DORA-asetus	Artikla 9	Ei sovelleta
COBIT 2019	DSS01.03, DSS05.01, MEA03	Ei sovelleta

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on määrittää organisaation vaatimukset sisäisten ja ulkoisten verkkojen suojaamiseksi luvattomalta käytöltä, palveluhäiriöiltä, tiedon sieppaukselta ja väärinkäytöltä.

1.2 Tällä politiikalla varmistetaan, että kaikki verkkoinfrastruktuuri, mukaan lukien fyysinen, virtuaalinen sekä pilvi- ja hybridiympäristöihin kuuluva infrastruktuuri, suojataan kerroksellisilla puolustusratkaisuilla, kuten segmentoinnilla, palomuureilla, turvallisella reitityksellä ja keskistetyllä valvonnalla.

1.3 Tämä politiikka toimeenpanee ISO/IEC 27001 -standardin kohdan 8.1 ja liitteen A kontrollit 8.20–8.22 sekä varmistaa sovellettavien lakisääteisten ja sääntelyyn perustuvien velvoitteiden noudattamisen EU:n GDPR:n 32 artiklan, EU:n NIS2-direktiivin 21 artiklan ja EU:n DORA-asetuksen 9 artiklan mukaisesti.

2. Soveltamisala

2.1 Tämä politiikka koskee kaikkia verkkoja ja niihin liittyviä infrastruktuurikomponentteja, mukaan lukien:

2.1.1 reitittimet, kytkimet, langattomat tukiasemat ja palomuurit

2.1.2 pilven virtuaaliverkot (esim. AWS VPC, Azure VNET), VPN-keskittimet ja SD-WAN-ratkaisut

2.1.3 sisäiset lähiverkot, demilitarisoidut vyöhykkeet (DMZ), etäkäyttöyhteydet sekä toimipisteiden väliset tai kolmansien osapuolten yhteydet

2.1.4 tukipalvelut, kuten DNS, DHCP, välityspalvelimet ja valvontalaitteet

2.2 Tämä politiikka on sitova kaikille henkilöille ja kolmansien osapuolten palveluntarjoajille, jotka hallinnoivat, konfiguroivat tai valvovat organisaation verkkoja tai liittyvät niihin riippumatta siitä, sijaitsevatko ne omissa tiloissa vai pilviympäristössä.

2.3 Kaikkien organisaation verkkoihin liitettyjen järjestelmien ja sovellusten on sijainnista tai omistajuudesta riippumatta täytettävä tämän politiikan verkkoturvallisuusvaatimukset.

3. Tavoitteet

3.1 Varmistaa verkkojen kautta siirrettävän tiedon luottamuksellisuus, eheys ja saatavuus vahvan pääsynhallinnan, turvallisen reitityksen ja valvonnan avulla.

3.2 Estää luvaton käyttö, sivuttaisliikkuminen ja verkkoon liitettyjen resurssien väärinkäyttö toteuttamalla segmentointi, vyöhykejako ja rajasuojaukset.

3.3 Ylläpitää johdonmukaisia verkkokonfiguraatioita toimialastandardien ja uhkatiedustelun perusteella muuttuvilta kyberuhkilta suojautumiseksi.

3.4 Suojata ulkoinen viestintä, pilvien välinen yhdistettävyys ja etäkäyttö salatuilla yhteyksillä, vahvalla todennuksella ja päätelaitteen tilan tarkistuksella.

3.5 Tuottaa näkyvyys verkkotoimintaan keskitetyn lokituksen, reaaliaikaisen verkkoliikenteen tarkastuksen ja automatisoitujen hälytysten avulla.

3.6 Varmistaa vaatimustenmukaisuus yhdenmukaistamalla kaikki verkkotoiminnot ISO/IEC 27001:2022:n, EU:n GDPR:n, EU:n NIS2-direktiivin, EU:n DORA-asetuksen ja COBIT 2019:n vaatimusten kanssa.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa, että se katselmoidaan ja pidetään yhdenmukaisena organisaation laajemman kyberturvallisuusstrategian kanssa.

4.1.2 Hyväksyy verkon segmentointimallit, arkaluonteisia järjestelmiä koskevat palomuurisääntökokonaisuudet ja poikkeuspyynnöt.

4.2 Verkkoturvallisuuspäällikkö / infrastruktuuriturvallisuudesta vastaava henkilö

4.2.1 Hallinnoi verkon suojausarkkitehtuuria, mukaan lukien palomuurit, tunkeutumisen havaitsemis- ja estojärjestelmät (IDS/IPS), VPN-yhteydet ja turvallinen reititys.

4.2.2 Vastaa verkon segmentoinnista, VLAN-määrityksistä, liikenteen vyöhykejaosta ja ulkoisista yhteyksistä.

4.2.3 Varmistaa saapuvan ja lähtevän liikenteen suodatuksen sekä Zero Trust -mallin toteutuksen jatkuvan katselmoinnin verkon eri tasoilla.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Verkkoturvallisuuspäällikön on katselmoitava tämä politiikka vuosittain yhteistyössä tietoturvajohtajan (CISO) kanssa, ja sitä on päivitettävä seuraavien perusteella:

9.1.1 kehittyvät uhkat (esim. uudet hyökkäystekniikat, protokollahaavoittuvuudet)

9.1.2 infrastruktuurimuutokset (esim. pilvimigraatiot, SD-WAN-käyttöönotot)

9.1.3 verkon suojaustoimiin vaikuttavat sääntely- tai standardimuutokset

9.1.4 auditointihavainnot, poikkeamatrendit tai kontrollien aiheuttama suorituskyvyn heikkeneminen

9.2 Katselmointi on käynnistettävä myös seuraavissa tilanteissa:

9.2.1 merkittävät muutokset verkkoarkkitehtuurissa

9.2.2 uusien palomuuri-, VPN- tai pilviverkkoalustojen käyttöönotto

9.2.3 keskeisten omaisuuserien tai luotettujen vyöhykkeiden käytöstäpoisto

9.3 Päivitykset on kirjattava ISMS:n asiakirjahallintarekisteriin ja niistä on tiedotettava seuraaville:

9.3.1 infrastruktuuri- ja verkko-operaatiot

9.3.2 SOC- ja tietoturvasuunnittelutiimit

9.3.3 sovellustiimit, joiden järjestelmät ovat riippuvaisia verkkovirroista

9.3.4 kaikki kolmannet osapuolet, joilla on aktiivinen yhteenliitettävyys

9.4 Kaikki politiikan aiemmat versiot on arkistoitava turvallisesti muutoshistoriamerkinnöin auditoinnin todennettavuuden ja muutosten jäljitettävyyden varmistamiseksi.

10. Liittyvät politiikat ja yhteydet

10.1 P1 - Tietoturvapolitiikka. Määrittää perustavanlaatuiset tietoturvaperiaatteet ja edellyttää kerroksellisia suojaustoimia, mukaan lukien verkkoon perustuvat pääsynhallinta- ja uhkienhallintakontrollit.

10.2 P4 - Pääsynhallintapolitiikka. Varmistaa, että verkon segmentointi toteutetaan yhdenmukaisesti käyttäjäroolien, vähimmän oikeuden periaatteen ja käyttöoikeuksien myöntämissääntöjen kanssa.

10.3 P5 - Muutoksenhallintapolitiikka. Sääntelee palomuurimuutoksia, VPN-sääntöjen muutoksia ja reititysmuutoksia dokumentoidun ja todennettavissa olevan prosessin kautta.

10.4 P12 - Omaisuudenhallintapolitiikka. Tukee verkkoon liitettyjen järjestelmien tunnistamista ja luokittelua sekä varmistaa, että kaikkia liitettyjä omaisuuseriä hallitaan politiikassa määritellyn soveltamisalan mukaisesti.

10.5 P22 - Lokitus- ja valvontapolitiikka. Ohjaa verkkolokien, mukaan lukien palomuuritapahtumien, käyttöyritysten ja poikkeamien havaitsemisen, keräämistä, korrelointia ja säilyttämistä.

10.6 P30 - Tietoturvapoikkeamien hallintapolitiikka. Määrittää eskalointi-, rajaamis- ja poistamismenettelyt verkon kautta välittyviin uhkiin tai tunkeutumisiin reagoimiseksi, kuten DDoS-hyökkäyksiin, sivuttaisliikkumiseen tai luvattomaan käyttöön.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukainen kansainvälisten standardien ja sääntelyvaatimusten kanssa, joissa määritellään turvalliset verkkotoiminnot, segmentointi, rajasuojaukset ja turvallinen etäkäyttö.

11.2 ISO/IEC 27001

11.2.1 Kohta 8.1 - Toiminnan suunnittelu ja ohjaus: edellyttää, että tekniset kontrollit, mukaan lukien verkon suojaustoimenpiteet, sisällytetään operatiivisiin prosesseihin.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrollit 8.20–8.22. Antaa ohjeita verkkojen suojaamiseen, palvelujen segmentointiin ja verkkopalvelujen suojaamiseen pääsynhallinnan ja valvonnan avulla.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Boundary Protection: edellyttää rajakontrolleja, segmentointia ja turvallisia yhteenliitäntöjä.

11.4.2 AC-4 - Information Flow Enforcement: tukee vyöhykejakoa ja sääntöpohjaisia liikenteen rajoituksia.

11.4.3 SC-32 - Information System Partitioning: edistää tietojärjestelmien loogista erottelua.

11.5 EU:n GDPR (2016/679)

11.5.1 Artikla 32 - käsittelyn turvallisuus: edellyttää teknisiä toimenpiteitä, kuten palomuureja ja segmentointia, henkilötietojen suojaamiseksi.

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

11.6.1 Artikla 21(2)(d): edellyttää tehokasta verkko- ja tietojärjestelmien turvallisuutta, rajasuojauksia, turvallista konfigurointia ja eriyttämiskontrolleja.

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

11.7.1 Artikla 9 - ICT-riskien hallinta: velvoittaa finanssialan toimijat suojaamaan verkot ja yhteenliitännät luvattomalta käytöltä, tietovuodoilta ja toiminnan häiriöiltä.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitor Infrastructure: edellyttää ennakoivaa verkon tilan ja yhdistettävyyden hallintaa.

11.8.2 DSS05.01 - Protect Against Malware: sisältää segmentoinnin ja rajakontrollit leviämisen minimoimiseksi.

11.8.3 MEA03 - Monitor, Evaluate and Assess Compliance: vahvistaa verkkopolitiikan soveltamista ja vaatimustenmukaisuuden arviointeja.