					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P34					Asiakirjan nimi: **Mobiililaitteita ja BYOD-käytäntöä koskeva politiikka**							
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 sääntelyn kanssa

Standardi/säädös	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Määrittää tietoturvakontrollit ja vaatimustenmukaisuusvaatimukset
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Sisältää yksityiskohtaiset kontrollit mobiililaitteiden hallintaan
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Mobiilikäytön käyttöoikeuksien hallinta, etäkäyttö, konfiguraatio ja tietoturvavaatimukset
EU:n GDPR	5(1)(f), 25, 32	Pakolliset vaatimukset tietosuojalle, tietojen salaukselle ja käsittelyn turvallisuudelle
EU:n NIS2-direktiivi	21(2)(d)	Mobiilikäytön tekniset ja organisatoriset suojatoimenpiteet
EU:n DORA-asetus	9, 10	TVT-riskienhallinta ja mobiilikäytön tietoturvavaatimukset
COBIT 2019	APO13.02, DSS01.04, BAI09	Tietoturvasuunnitelmat, omaisuuserien konfiguraatio ja mobiiliympäristöjen kontrollit

1. Tarkoitus

1.1 Tämä politiikka määrittää tietoturva-, vaatimustenmukaisuus- ja toiminnalliset vaatimukset mobiililaitteiden ja henkilökohtaisten laitteiden (BYOD, Bring Your Own Device) käytölle, kun niillä käytetään organisaation järjestelmiä, sovelluksia tai tietoja.

1.2 Politiikan tarkoituksena on varmistaa yrityksen tietojen luottamuksellisuus, eheys ja saatavuus, kun tietoja käytetään tai käsitellään mobiilipäätelaitteilla, mukaan lukien älypuhelimet, tabletit, kannettavat tietokoneet ja hybridilaitteet.

1.3 Tässä politiikassa määritetään myös tekniset ja menettelylliset kontrollit, joita tarvitaan esimerkiksi tietovuodon, luvattoman käytön, laitteen katoamisen tai varkauden sekä mobiilisovellusten vaarantumisen riskien pienentämiseksi.

1.4 Tämä politiikka tukee sääntely- ja sopimusvelvoitteiden noudattamista sekä mahdollistaa turvallisen mobiilityöskentelyn työntekijöille, toimeksisaajille ja valtuutetuille kolmansille osapuolille.

2. Soveltamisala

2.1 Tämä politiikka koskee koko henkilöstöä, mukaan lukien työntekijät, toimeksisaajat, harjoittelijat ja kolmansien osapuolten palveluntarjoajat, jotka käyttävät mobiililaitteita yrityksen tietojen, järjestelmien, sovellusten tai viestintäalustojen käyttöön.

2.2 Politiikka kattaa kaikki mobiilit tietojenkäsittelylaitteet, mukaan lukien seuraavat:

2.2.1 Älypuhelimet ja tabletit (iOS, Android jne.)

2.2.2 Kannettavat tietokoneet ja ultrabookit (Windows, macOS, Linux)

2.2.3 Puettavat laitteet ja hybridiälylaitteet, jotka kykenevät synkronoimaan tietoja

2.3 Tätä politiikkaa sovelletaan riippumatta siitä, onko laite yrityksen omistama vai käyttäjän henkilökohtainen BYOD-sopimuksen piiriin kuuluva laite.

2.4 Politiikka kattaa kaikki käyttöyhteydet, mukaan lukien VPN-yhteydet, virtuaalityöpöydät, pilvisovellukset, sähköpostin, yhteistyöalustat (esim. SharePoint, Teams) ja tiedostojen synkronointityökalut (esim. OneDrive, Dropbox, jos hyväksytty).

2.5 Politiikka koskee käyttöä etätyössä, organisaation tiloissa, matkustettaessa ja hybridityössä.

3. Tavoitteet

3.1 Pienentää tietojen vaarantumisen, tietovuodon tai tietojen menetyksen riskiä, joka aiheutuu mobiililaitteiden turvattomasta käytöstä.

3.2 Varmistaa yhdenmukaisten ja toimeenpantavien tietoturvakontrollien soveltaminen kaikkiin mobiilipäätelaitteisiin omistusmallista riippumatta (yrityksen omistama tai BYOD).

3.3 Varmistaa, että mobiililaitteiden käyttö täyttää ISO/IEC 27001 -standardin sekä muiden tietosuojaan, tietojen suojaamiseen ja kyberturvallisuuteen sovellettavien sääntelykehysten vaatimukset.

3.4 Mahdollistaa mobiililaitteiden turvallinen integrointi organisaation toiminta-, viestintä- ja yhteistyöprosesseihin.

3.5 Määrittää selkeät vastuut ja menettelyt mobiililaitehallinnalle (MDM), mukaan lukien rekisteröinti, etätyhjennys, salaus, tunnistautuminen ja seuranta.

3.6 Suojata omia laitteitaan käyttävien henkilöiden yksityisyyttä samalla, kun turvataan organisaation arkaluonteiset tiedot.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO) / IT-tietoturvasta vastaava henkilö

4.1.1 Määrittää mobiililaitteiden ja BYOD-käytön politiikan sekä tekniset standardit.

4.1.2 Valvoo mobiililaitteisiin liittyvien kontrollien vaatimustenmukaisuutta, poikkeamien hallintaa ja tietoturvaloukkausten käsittelyä.

4.1.3 Tekee yhteistyötä lakiasioiden ja henkilöstöhallinnon kanssa varmistaakseen, että politiikan soveltaminen on oikeudellisesti kestävää ja organisaation toimintatapojen mukaista.

4.2 Tietohallinnon järjestelmänvalvoja / MDM-järjestelmänvalvoja

4.2.1 Hallinnoi mobiililaitteiden käyttöönottoa, rekisteröintiä ja konfigurointia MDM-ratkaisujen avulla.

4.2.2 Toteuttaa laitetason kontrollit (esim. salaus, PIN-koodit, sovelluskontrollit).

4.2.3 Toteuttaa tarvittaessa etätyhjennyksen, laitteen lukituksen ja käyttöoikeuksien peruutuksen.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 CISO:n tai nimetyn tietoturvapäällikön on katselmoitava tämä politiikka vähintään vuosittain varmistaakseen yhdenmukaisuuden seuraavien kanssa:

9.1.1 Muutokset mobiilikäyttöjärjestelmissä, MDM-teknologioissa tai tunnistautumisstandardeissa

9.1.2 Mobiilitietojen suojaamiseen vaikuttavat sääntelyyn tai sopimuksiin liittyvät muutokset (esim. GDPR, DORA, NIS2)

9.1.3 ISO/IEC 27001:2022-, ISO/IEC 27002:2022- tai NIST SP 800-53 Rev.5 -kontrollikokonaisuuksien muutokset

9.1.4 Auditointien, tietoturvaloukkausten jälkikäsittelyjen tai henkilöstön ilmoitusten palaute

9.2 Välikatselmointeja voidaan käynnistää seuraavien perusteella:

9.2.1 Mobiililaitteisiin tai BYOD-alustoihin liittyvät tietoturvaloukkaukset

9.2.2 Toimittajan ilmoitus tuetuissa alustoissa havaituista korkean riskin haavoittuvuuksista

9.2.3 Uusien liiketoiminnassa käytettävien mobiilisovellusten tai yhteistyöalustojen käyttöönotto

9.3 Politiikan päivitykset on:

9.3.1 Dokumentoitava politiikan versiohistoriaan

9.3.2 Viestittävä koko henkilöstölle ja vaikutuksen piirissä oleville toimeksisaajille

9.3.3 Vahvistettava uudelleen päivitettynä kuittauksena kaikilta BYOD-käyttäjiltä

9.4 Kaikki katselmoinnit ja muutokset on hyväksyttävä muodollisesti ylimmän johdon toimesta ja kirjattava politiikan muutosrekisteriin.

10. Liitännäiset politiikat ja kytkennät

10.1 Tämä politiikka on riippuvuussuhteessa useisiin organisaation ISMS-viitekehyksen keskeisiin politiikkoihin. Keskeiset kytkennät ovat:

10.1.1 P1 – Tietoturvapolitiikka: Määrittää kaikkiin tietoturvakontrolleihin sovellettavat yleiset hallintaperiaatteet, mukaan lukien mobiililaitteiden käyttöä koskevat kontrollit.

10.1.2 P3 – Hyväksyttävän käytön politiikka: Määrittää teknologian käyttöön liittyvät sallitut toimintatavat ja rajoitukset, joita sovelletaan suoraan mobiili- ja BYOD-käyttöön.

10.1.3 P9 – Etätyöpolitiikka: Määrittää mobiileihin työympäristöihin liittyvät lisätietoturvavelvoitteet ja täydentää tässä politiikassa määritettyjä mobiilikohtaisia kontrolleja.

10.1.4 P13 – Tietojen luokittelu- ja merkintäpolitiikka: Määrittää, miten mobiililaitteilla olevia tietoja on käsiteltävä luokitustason perusteella, mikä vaikuttaa tallennukseen, siirtoon ja salauksen toteuttamiseen.

10.1.5 P22 – Lokitus- ja seurantapolitiikka: Tukee mobiilikäytön lokien keräämistä ja katselmointia poikkeamien tai rikkomusten havaitsemiseksi.

10.1.6 P30 – Tietoturvaloukkausten hallintapolitiikka: Määrittää, miten mobiiliin liittyvät tapahtumat (esim. laitteen katoaminen, luvaton käyttö) käsitellään ja eskaloidaan.

10.1.7 P33 – Auditointi- ja vaatimustenmukaisuuden seurantapolitiikka: Määrittää perustan mobiilitietoturvan vaatimustenmukaisuuden säännöllisille tarkastuksille, mukaan lukien BYOD-politiikan noudattamisen seuranta.

11. Viitestandardit ja viitekehykset

11.1 Tämä politiikka on yhdenmukaistettu kansainvälisesti tunnustettujen kyberturvallisuuden viitekehysten ja oikeudellisten velvoitteiden kanssa, jotta mobiililaitteiden ja henkilökohtaisten BYOD-laitteiden turvallinen käyttö yritysympäristössä voidaan varmistaa.

11.2 ISO/IEC 27001:

11.2.1 Kohta 5.10 – Tietojen ja muiden omaisuuserien hyväksyttävä käyttö: Edellyttää kontrolleja yrityksen omaisuuserien, mukaan lukien mobiililaitteiden, vastuulliselle käytölle.

11.2.2 Kohta 5.11 – Etätyö: Määrittää turvalliset käytännöt, kun järjestelmiä käytetään yrityksen toimitilojen ulkopuolelta.

11.2.3 Kohta 5.12 – Mobiililaitteiden käyttö: Edellyttää riskiperusteisia kontrolleja mobiilipäätelaitteille ja BYOD-konfiguraatioille.

11.2.4 Kohta 5.13 – Tiedonsiirto: Edellyttää mobiilikanavien kautta siirrettävien tietojen suojaamista.

11.3 ISO/IEC 27002:2022 – Kontrollit 5.10–5.13:

11.3.1 Liitteen A kontrollit 5.10–5.13: Määrittävät, miten mobiilikäyttö, salaus, seuranta ja häviämiseen liittyvien riskien pienentäminen on toteutettava ISMS-järjestelmässä. Nämä kontrollit antavat yksityiskohtaiset toteutusohjeet mobiilipäätelaitteiden suojaamiseen, kontituksen toteuttamiseen, laitteen eheyden seurantaan ja BYOD-käytön tietosuojaa huomioiviin konfiguraatioihin.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Mobiililaitteiden käyttöoikeuksien hallinta: Määrittää perustason suojaukset, mukaan lukien salaus, tunnistautuminen ja MDM-valvonta.

11.4.2 AC-17 – Etäkäyttö: Edellyttää suojattua tunnistautumista ja istunnon suojausta etäkäyttöä käyttäville mobiilikäyttäjille.

11.4.3 CM-7 – Vähimmäistoiminnallisuus: Tukee tarpeettomien sovellusten ja ominaisuuksien poistamista mobiilipäätelaitteista riskin pienentämiseksi.

11.4.4 MP-5 – Tietovälineiden siirron suojaus: Määrittää tietojen turvallisen siirtämisen mobiilijärjestelmistä ulkoisiin tai pilvikohteisiin.

11.4.5 SC-12 – Salausavainten muodostaminen: Edellyttää turvallisten salausprotokollien käyttöä mobiiliviestinnässä ja tallennuksessa.

11.5 EU:n GDPR (2016/679):

11.5.1 Artikla 5(1)(f) – Eheys ja luottamuksellisuus: Edellyttää organisaatioiden suojaavan mobiililaitteilla olevat henkilötiedot luvattomalta tai lainvastaiselta käytöltä.

11.5.2 Artikla 25 – Sisäänrakennettu ja oletusarvoinen tietosuoja: Edellyttää, että tietosuoja sisällytetään BYOD- ja MDM-menettelyihin.

11.5.3 Artikla 32 – Käsittelyn turvallisuus: Edellyttää riskiperusteisia kontrolleja (esim. salaus, tunnistautuminen, käyttöoikeuksien hallinta) henkilötietojen suojaamiseksi mobiilialustoilla.

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

11.6.1 Artikla 21(2)(d): Edellyttää, että kriittisten järjestelmien ja tietojen mobiilikäyttö suojataan asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, kuten päätelaitehallinnalla, salauksella ja seurannalla.

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

11.7.1 Artikla 9 – TVT-riskienhallintakehys: Edellyttää finanssialan toimijoita pienentämään mobiili- ja etäkäyttöön liittyviä riskejä osana operatiivista häiriönsietokykyä.

11.7.2 Artikla 10 – TVT-järjestelmien tietoturvavaatimukset: Edellyttää turvallista mobiiliarkkitehtuuria sekä mobiililähtöisten kyberuhkien seurantaa ja vastekykyä.

11.8 COBIT 2019:

11.8.1 APO13.02 – Tietoturvasuunnitelman laatiminen ja ylläpito: Edellyttää, että mobiililaitteiden käyttö, mukaan lukien BYOD, integroidaan organisaation tietoturvastrategioihin.

11.8.2 DSS01.04 – Omaisuuserien konfiguraation ja eheyden hallinta: Soveltuu mobiililaitteiden konfiguraation hallintaan ja turvalliseen käyttöönottoon.

11.8.3 BAI09.01 – Kontrollien määrittäminen ja ylläpito: Tukee teknisten ja menettelyllisten suojausten toteuttamista turvallisiin mobiili- ja etätoimintoihin.