					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P34S					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**

Yhdenmukaistettu standardien ja sääntelyn kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohdat 5.1, 5.2, 6.1, 6.2, 8	Tietoturvan hallintajärjestelmän (ISMS) yleiset vaatimukset sekä mobiililaitteita ja BYOD-käytäntöä koskevat hallintatoimenpiteet
ISO/IEC 27002:2022	Hallintatoimenpiteet 5.10–5.13	Yksityiskohtaiset hallintatoimenpiteet mobiililaitteille, BYOD-käytölle ja etäyhteyksille
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Liittovaltion vaatimukset laitteiden, tallennusvälineiden ja määritysten hallintatoimenpiteille
EU:n GDPR	Artikla 5(1)(f)	Henkilötietojen suojaus mobiilipäätelaitteissa
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Liiketoiminnan kannalta kriittisten laitteiden suojaus, mukaan lukien BYOD
EU:n DORA-asetus	Artiklat 9, 10	TVT-riskien hallinta ja jatkuvuus mobiilipäätelaitteiden osalta
COBIT 2019	APO13, DSS01, DSS05	IT-hallinto, operatiivinen toiminta ja tietoturvapalvelujen hallintatoimenpiteet

1. Tarkoitus

1.1. Tässä politiikassa määritellään pakolliset tietoturvavaatimukset mobiililaitteiden, mukaan lukien älypuhelimien, tablettien ja kannettavien tietokoneiden, käytölle silloin, kun niillä käytetään yrityksen tietoja, järjestelmiä tai palveluja.

1.2. Politiikka säätelee myös omien laitteiden käyttöä työssä (BYOD), jotta asiakkaiden ja liiketoiminnan tiedot suojataan laitteen omistajasta riippumatta.

1.3. Tällä politiikalla varmistetaan yhdenmukaiset suojatoimenpiteet mobiilikäytölle, tuetaan ISO/IEC 27001 -sertifiointitavoitteiden saavuttamista ja ehkäistään tietojen menetystä tai vaarantumista kadonneiden, varastettujen tai väärinkäytettyjen mobiilipäätelaitteiden seurauksena.

1.4. Politiikalla varmistetaan, että pk-yrityksissä ilman erillistä IT-tiimiä mobiilikäyttöön sovelletaan teknisiä ja menettelyllisiä suojatoimenpiteitä, mukaan lukien etätyöympäristöt ja pilvipalvelut.

2. Soveltamisala

2.1. Tätä politiikkaa sovelletaan kaikkiin työntekijöihin, toimeksisaajiin, harjoittelijoihin ja palveluntarjoajiin, jotka:

2.1.1. käyttävät mobiililaitetta yrityksen tietojen tai järjestelmien käyttämiseen, käsittelyyn tai tallentamiseen

2.1.2. muodostavat VPN-yhteyden kautta yhteyden yrityksen palveluihin, mukaan lukien sähköposti, jaetut kansiot, pilvisovellukset tai sisäiset järjestelmät

2.2. Politiikka kattaa:

2.2.1. kaikki mobiililaitteet: älypuhelimet, tabletit ja kannettavat tietokoneet (yrityksen toimittamat tai henkilökohtaiset BYOD-laitteet)

2.2.2. kaikki käyttöjärjestelmät (esim. iOS, Android, Windows, macOS)

2.2.3. kaikki sijainnit (toimisto, koti, etätyö, julkiset tilat)

2.3. Tätä politiikkaa sovelletaan kaikkiin työympäristöihin, ja sitä on noudatettava laitteen omistussuhteesta riippumatta.

3. Tavoitteet

3.1. Estää tietojen menetys: varmistaa, ettei mobiilikäyttö altista arkaluonteisia yrityksen tai asiakkaiden tietoja oikeudettomalle käytölle, varkaudelle tai väärinkäytölle.

3.2. Määrittää selkeät säännöt BYOD-käytölle: asettaa toimeenpantavat ehdot henkilökohtaisten laitteiden käytölle työssä sekä varmistaa oikeudelliset ja tekniset suojatoimenpiteet.

3.3. Tukea vaatimustenmukaisuutta: täyttää ISO/IEC 27001:n, EU:n GDPR:n, EU:n NIS2-direktiivin ja muiden velvoitteiden vaatimukset toimeenpantavien mobiilitietoturvakäytäntöjen avulla.

3.4. Minimoida operatiivinen riski: vähentää mobiililaitteiden väärinkäytöstä, vaarantumisesta tai toimintahäiriöstä aiheutuvan operatiivisen häiriön todennäköisyyttä.

3.5. Ylläpitää asiakkaiden luottamusta: osoittaa asiakkaille ja kumppaneille, että heidän tietonsa pysyvät suojattuina myös silloin, kun niitä käytetään mobiili- tai henkilökohtaisilla laitteilla.

4. Roolit ja vastuut

4.1. Toimitusjohtaja:

4.1.1. vastaa tästä politiikasta.

4.1.2. hyväksyy kaiken mobiili- ja BYOD-käytön yrityksen järjestelmiin.

4.1.3. varmistaa, että BYOD-sopimukset allekirjoitetaan, säilytetään ja niiden noudattamista seurataan.

4.1.4. varmistaa, että ulkoiset IT-palveluntarjoajat toteuttavat vaaditut mobiililaitteiden suojatoimenpiteet.

4.2. Nimetty henkilöstö tai IT-tuki:

4.2.1. avustaa työssä käytettävien mobiililaitteiden käyttöönotossa, rekisteröinnissä ja määrityksessä.

4.2.2. toteuttaa mobiilikäyttöön liittyvät käyttöoikeuksien hallinnan keinot, sovellusrajoitukset ja seurantavaatimukset.

4.2.3. tukee mobiililaitteisiin liittyvien tietoturvapoikkeamien käsittelyä (kadonneet, varastetut tai vaarantuneet laitteet).

[... 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 12 kuukaudessa.

9.1.2. katselmoinnissa on varmistettava jatkuva yhdenmukaisuus ISO/IEC 27001:n vaatimusten, kehittyvien mobiiliteknologioiden ja liiketoiminnan muutosten kanssa.

9.1.3. päivityksissä on otettava huomioon myös viimeaikaiset poikkeamat, auditointien tulokset ja sääntelykehitykset (esim. EU:n GDPR, EU:n NIS2-direktiivi, DORA-asetus).

9.2. Välikatselmoinnin käynnistävät tapahtumat

9.2.1. tämä politiikka on päivitettävä välittömästi, jos jokin seuraavista toteutuu:

9.2.1.1. merkittävä mobiilitietoturvapoikkeama (esim. kadonneen tai murretun laitteen kautta tapahtunut tietomurto)

9.2.1.2. muutos tuetuissa alustoissa tai mobiililaitteiden hallintatyökaluissa

9.2.1.3. henkilökohtaisten laitteiden käyttöön tai tietosuojaan vaikuttava lakisääteinen tai sääntelymuutos

9.2.1.4. uusien sovellusten, palvelujen tai kolmansien osapuolten työkalujen käyttöönotto mobiililaitteissa

9.3. Muutosten dokumentointi

9.3.1. kaikki katselmoinnit ja päivitykset on dokumentoitava, mukaan lukien katselmoinnin päivämäärä, tehdyt muutokset ja toimitusjohtajan hyväksyntä.

9.3.2. versiohallintahistoria on säilytettävä auditointitarkoituksia varten.

9.4. Viestintä ja saatavuus

9.4.1. toimitusjohtajan on varmistettava, että kaikille käyttäjille (työntekijät, toimeksisaajat, kolmannet osapuolet) tiedotetaan muutoksista.

9.4.2. päivitetyt versiot on saatettava helposti saataville esimerkiksi jaettuihin kansioihin tai sisäisille alustoille.

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka on osa pk-yrityksen tietoturvapolitiikkojen kokonaisuutta, ja sitä on toteutettava yhdessä seuraavien politiikkojen kanssa:

10.1.1. P4S – Käyttöoikeuksien hallintapolitiikka: määrittelee vaatimukset järjestelmien turvallisen käytön hallinnalle, mukaan lukien mobiililaitteilla käytettävät järjestelmät. Edellyttää hyvää salasanojen hallintaa ja istunnon hallintatoimenpiteitä.

10.1.2. P8S – Tietoturvatietoisuuden ja koulutuksen politiikka: varmistaa, että käyttäjät koulutetaan mobiililaitteiden turvalliseen käyttöön, poikkeamien ilmoittamiseen ja BYOD-käytön ehtoihin.

10.1.3. P17S – Tietosuojan ja yksityisyyden politiikka: määrittää EU:n GDPR:n mukaisen henkilö- ja yritystietojen käsittelyn mobiilialustoilla erityisesti silloin, kun työssä käytetään henkilökohtaisia laitteita.

10.1.4. P9S – Etätyöpolitiikka: yhdenmukaistaa mobiilikäyttöä koskevat vaatimukset etätyössä tai kotona työskenneltäessä, mukaan lukien laitteiden käsittely ja verkkoyhteyksien suojatoimenpiteet.

10.1.5. P30S – Poikkeamien hallintapolitiikka: määrittää toimintamallin mobiililaitteisiin liittyvien poikkeamien käsittelyyn, mukaan lukien vaarantuneet tai kadonneet laitteet.

10.2. Nämä liittyvät politiikat muodostavat yhdessä kattavan hallintatoimenpiteiden kokonaisuuden mobiililaitteiden tietoturvalle pk-yrityksissä, joissa ei ole erillistä IT-henkilöstöä, ja varmistavat toimeenpantavuuden, läpinäkyvyyden ja sertifiointivalmiuden.

11. Viitestandardeja ja viitekehyksiä

11.1. Tämä politiikka tukee täysimääräistä yhdenmukaisuutta seuraavien tietoturva- ja vaatimustenmukaisuusstandardien kanssa:

11.2. ISO/IEC 27001:

11.2.1. Kohta 5.1 – Johtajuus ja sitoutuminen: varmistaa johdon valvonnan ja vastuun mobiili- ja BYOD-käytöstä

11.2.2. Kohta 6.1 – Toimenpiteet riskien käsittelemiseksi: edellyttää mobiilitietoturvariskien arviointia ja käsittelyä

11.2.3. Kohta 8.1 – Toiminnan suunnittelu ja ohjaus: edellyttää yhdenmukaisia mobiilikäytön menettelyjä liiketoimintatietojen suojaamiseksi

11.3. ISO/IEC 27002:

11.3.1. Hallintatoimenpiteet 5.10 (mobiililaitteiden käyttö), 5.11 (etätyö), 5.12 (etäkäyttö) ja 5.13 (BYOD): antavat toteutusohjeita laiteriskien hallintaan pienyritysympäristössä

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Mobiililaitteiden käyttöoikeuksien hallinta: edellyttää tietoturva-asetuksia hyväksytylle mobiilikäytölle

11.4.2. AC-20 – Ulkoisten järjestelmien käyttö: ohjaa BYOD-käyttöön ja etäyhteyksiin liittyviä riskejä

11.4.3. CM-6 – Konfiguraatioasetukset: edellyttää turvallisia oletus- ja mukautettuja asetuksia mobiilialustoilla

11.4.4. MP-7 – Tallennusvälineiden käyttö: käsittelee mobiilitallennuksen ja tietojen käytön asianmukaista käyttöä ja rajoituksia

11.5. EU:n GDPR (2016/679):

11.5.1. Artikla 5(1)(f) – Eheys ja luottamuksellisuus: edellyttää henkilötietojen suojaamista asianmukaisilla turvatoimilla erityisesti mobiilialustoilla

11.5.2. Artikla 32 – Käsittelyn turvallisuus: velvoittaa käyttämään asianmukaisia teknisiä ja organisatorisia toimenpiteitä mobiililaitteilla käytettävien tai tallennettavien tietojen suojaamiseksi

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

11.6.1. Artikla 21(2)(d) – Laitteiden tietoturvatoimenpiteet: edellyttää tietoturvan hallintatoimenpiteitä laitteistoille ja ohjelmistoille, joilla käytetään kriittisiä liiketoimintajärjestelmiä, mukaan lukien henkilökohtaiset laitteet

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

11.7.1. Artikla 9 – TVT-riskien hallintakehys: edellyttää kriittisessä liiketoimintaviestinnässä ja pilvipalveluissa käytettävien mobiilipäätelaitteiden suojaamista

11.7.2. Artikla 10 – TVT-liiketoiminnan jatkuvuus: edellyttää yritysjärjestelmien jatkuvaa turvallista käyttöä myös häiriötilanteissa ja etätyössä

11.8. COBIT 2019:

11.8.1. APO13 – Tietoturvan hallinta: edellyttää organisaatiolta yrityksen riskeihin yhdenmukaistettujen mobiili- ja BYOD-politiikkojen soveltamista

11.8.2. DSS01 – Operatiivisen toiminnan hallinta: varmistaa turvallisten käyttömekanismien teknisen toteutuksen

11.8.3. DSS05 – Tietoturvapalvelujen hallinta: ohjaa kolmansien osapuolten osallistumista turvallisten mobiiliympäristöjen ylläpitoon ja poikkeamien käsittelyn koordinointiin