					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P34					Dokumendi pealkiri: **Mobiilseadmete ja BYOD-poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatiivsete nõuetega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Rakendab turbekontrolle ja vastavusnõudeid
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Sätestab mobiilseadmete halduse üksikasjalikud kontrollimeetmed
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Juurdepääsukontrolli, kaugjuurdepääsu, konfiguratsiooni ja mobiilse kasutuse turbenõuded
ELi isikuandmete kaitse üldmäärus (GDPR)	5(1)(f), 25, 32	Kohustuslikud nõuded andmekaitsele, andmete krüptimisele ja töötlemise turvalisusele
ELi NIS2	21(2)(d)	Mobiilse juurdepääsu tehnilised ja korralduslikud kaitsemeetmed
ELi DORA	9, 10	IKT-riski juhtimise ja mobiilse kasutuse turbenõuded
COBIT 2019	APO13.02, DSS01.04, BAI09	Infoturbeplaanid, varade konfiguratsioon ja kontrollimeetmed mobiilsetes keskkondades

1. Eesmärk

1.1 Käesolev poliitika sätestab turbe-, vastavus- ja tegevusnõuded mobiilseadmete ning isiklike tehnoloogiaseadmete kasutamiseks (oma seadme kasutamine (BYOD)) organisatsiooni süsteemidele, rakendustele või andmetele juurdepääsul.

1.2 Poliitika eesmärk on tagada ettevõtte teabe konfidentsiaalsus, terviklus ja käideldavus, kui teabele pääsetakse ligi või seda töödeldakse mobiilsete lõppseadmete kaudu, sealhulgas nutitelefonides, tahvelarvutites, sülearvutites ja hübriidseadmetes.

1.3 Samuti kehtestab see tehnilised ja protseduurilised kontrollimeetmed, mis on vajalikud selliste riskide maandamiseks nagu andmeleke, loata juurdepääs, seadme kaotsiminek või vargus ning mobiilirakenduste kompromiteerimine.

1.4 Käesolev poliitika toetab regulatiivset ja lepingulist vastavust ning võimaldab töötajatele, töövõtjatele ja volitatud kolmandatele isikutele turvalist mobiilset töökorraldust.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kogu personalile, sealhulgas töötajatele, töövõtjatele, praktikantidele ja kolmandatest isikutest teenuseosutajatele, kes kasutavad mobiilseadmeid ettevõtte andmetele, süsteemidele, rakendustele või suhtlusplatvormidele juurdepääsuks.

2.2 Poliitika hõlmab kõiki mobiilseid andmetöötlusseadmeid, sealhulgas, kuid mitte ainult:

2.2.1 nutitelefonid ja tahvelarvutid (iOS, Android jne);

2.2.2 sülearvutid ja ultrabook'id (Windows, macOS, Linux);

2.2.3 kantavad seadmed ja hübriidsed nutiseadmed, mis võimaldavad andmete sünkroniseerimist.

2.3 Poliitika kehtib sõltumata sellest, kas seade kuulub ettevõttele või on isiklik seade, mida kasutatakse BYOD-kokkuleppe alusel.

2.4 Poliitika hõlmab kõiki juurdepääsuviise, sealhulgas VPN-i, virtuaaltöölaua taristut (VDI), pilverakendusi, e-posti, koostööplatvorme (nt SharePoint, Teams) ja failide sünkroonimise tööriistu (nt OneDrive, Dropbox, kui need on volitatud).

2.5 Poliitika hõlmab kasutust kaugtöö, ettevõtte ruumides töötamise, reisimise või hübriidtöö korralduse puhul.

3. Eesmärgid

3.1 Vähendada ebaturvalisest mobiilseadmete kasutusest tulenevat andmete kompromiteerimise, andmelekkega või andmekaoga seotud riski.

3.2 Tagada järjepidevad ja rakendatavad turbekontrollid kõigis mobiilsetes lõppseadmetes, sõltumata omandimudelist (ettevõtte seade või BYOD).

3.3 Tagada, et mobiilseadmete kasutus vastab standardile ISO/IEC 27001 ning teistele andmekaitse, teabe kaitse ja küberturbega seotud kohaldatavatele regulatiivsetele raamistikele.

3.4 Võimaldada mobiilseadmete turvaline lõimimine organisatsiooni tegevus-, suhtlus- ja koostöötöövoogudesse.

3.5 Määratleda selged vastutused ja protsessid mobiilseadmete halduseks (MDM), sealhulgas registreerimine, kaugkustutus, krüptimine, autentimine ja seire.

3.6 Kaitsta oma seadmeid kasutavate isikute andmekaitsealaseid õigusi, tagades samal ajal organisatsiooni tundliku teabe kaitse.

4. Rollid ja vastutused

4.1 Infoturbejuht (CISO) / IT-turbejuht

4.1.1 Määratleb mobiilseadmete ja BYOD-i kasutamise poliitika ning tehnilised standardid.

4.1.2 Teostab järelevalvet mobiilseadmete kontrollimeetmete vastavuse, intsidentidele reageerimise ja erandite haldamise üle.

4.1.3 Koordineerib koostööd õigus- ja vastavusfunktsiooni ning personaliosakonnaga (HR), et tagada rakendamise õiguslik põhjendatus ja kooskõla organisatsiooni töökorraldusega.

4.2 Infotehnoloogia (IT) administraator / MDM-administraator

4.2.1 Haldab mobiilseadmete juurdepääsuõiguste andmist, registreerimist ja konfiguratsiooni MDM-lahenduste kaudu.

4.2.2 Rakendab seadmetaseme kontrollimeetmeid (nt krüptimine, PIN-koodid, rakenduste kontroll).

4.2.3 Teostab vajaduse korral kaugkustutuse, seadme lukustamise ja juurdepääsuõiguste tühistamise.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata infoturbejuhi või määratud infoturbejuhiga, et tagada kooskõla järgmisega:

9.1.1 muudatused mobiilsetes operatsioonisüsteemides, MDM-tehnoloogiates või autentimisstandardites;

9.1.2 regulatiivsed või lepingulised muudatused, mis mõjutavad mobiilsete andmete kaitset (nt GDPR, DORA, NIS2);

9.1.3 muudatused standardi ISO/IEC 27001:2022, ISO/IEC 27002:2022 või NIST SP 800-53 Rev.5 kontrollikomplektides;

9.1.4 auditite, intsidendijärgsete analüüside või töötajate teadete tulemused.

9.2 Vahepealsed ülevaatused võivad olla algatatud järgmistel juhtudel:

9.2.1 turvaintsidendid, mis hõlmavad mobiilseadmeid või BYOD-platvorme;

9.2.2 tarnija teavitus toetatud platvormide kõrge riskiga haavatavuste kohta;

9.2.3 uute mobiilirakenduste või koostööplatvormide kasutuselevõtt äritegevuses.

9.3 Poliitikauuendused peavad olema:

9.3.1 dokumenteeritud poliitika versiooniajaloos;

9.3.2 edastatud kogu personalile ja mõjutatud töövõtjatele;

9.3.3 uuendatud kinnitusega uuesti kinnitatud kõigi BYOD-kasutajate poolt.

9.4 Kõik läbivaatused ja muudatused tuleb ametlikult heaks kiita tippjuhtkonna poolt ning logida poliitikamuudatuste registris.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on vastastikku seotud organisatsiooni ISMS-raamistiku mitme olulise poliitikaga. Olulisemad seosed on järgmised:

10.1.1 P1 – Infoturbepoliitika: sätestab kõigi infoturbe kontrollimeetmete, sealhulgas mobiilseadmete kasutust reguleerivate kontrollide üldised juhtimispõhimõtted.

10.1.2 P3 – IT-vahendite lubatud kasutuse poliitika: määratleb tehnoloogia kasutamise lubatud käitumise ja piirangud, mis kehtivad vahetult ka mobiilseadmete ja BYOD-juurdepääsu puhul.

10.1.3 P9 – Kaugtööpoliitika: käsitleb mobiilsete töökeskkondade täiendavaid turvakohustusi ning täiendab käesolevas poliitikas määratletud mobiilispetsiifilisi kontrollimeetmeid.

10.1.4 P13 – Andmete klassifitseerimise ja märgistamise poliitika: reguleerib, kuidas mobiilseadmetes olevaid andmeid tuleb käsitleda vastavalt klassifitseerimistasemele, mõjutades säilitamist, edastamist ja krüptimise rakendamist.

10.1.5 P22 – Logimis- ja seirepoliitika: toetab mobiilse juurdepääsu logide kogumist ja läbivaatamist anomaaliate või rikkumiste tuvastamiseks.

10.1.6 P30 – Intsidentidele reageerimise poliitika: reguleerib mobiilseadmetega seotud intsidentide (nt seadme kaotsiminek, loata juurdepääs) käsitlemist ja eskaleerimist.

10.1.7 P33 – Auditi ja nõuetele vastavuse seire poliitika: loob aluse mobiilse turbe vastavuse perioodilisteks kontrollideks, sealhulgas BYOD-poliitika järgimise hindamiseks.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud küberturbe raamistike ja õiguslike kohustustega, et tagada mobiilseadmete ja isiklike tehnoloogiaseadmete (BYOD) turvaline kasutamine ettevõtte keskkondades.

11.2 ISO/IEC 27001:

11.2.1 Punkt 5.10 – Teabe ja varade lubatud kasutamine: nõuab kontrollimeetmeid ettevõtte varade, sealhulgas mobiilseadmete vastutustundlikuks kasutamiseks.

11.2.2 Punkt 5.11 – Kaugtöö: reguleerib turvalisi töövõtteid süsteemidele juurdepääsuks väljaspool ettevõtte ruume.

11.2.3 Punkt 5.12 – Mobiilseadmete kasutamine: nõuab riskipõhiseid kontrollimeetmeid mobiilsete lõppseadmete ja BYOD-konfiguratsioonide jaoks.

11.2.4 Punkt 5.13 – Teabe edastamine: nõuab mobiilsete kanalite kaudu edastatava teabe kaitset.

11.3 ISO/IEC 27002:2022 – kontrollimeetmed 5.10 kuni 5.13:

11.3.1 Lisa A kontrollimeetmed 5.10 kuni 5.13: täpsustavad, kuidas mobiilne juurdepääs, krüptimine, seire ja kaotsimineku mõju vähendamine tuleb ISMS-is rakendada. Need kontrollimeetmed annavad üksikasjalikud rakendusjuhised mobiilsete lõppseadmete kaitsmiseks, konteineriseerimise jõustamiseks, seadme tervikluse seireks ja andmekaitset arvestavate BYOD-konfiguratsioonide tagamiseks.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Juurdepääsukontroll mobiilseadmetele: määratleb baaskaitsemeetmed, sealhulgas krüptimise, autentimise ja MDM-i rakendamise.

11.4.2 AC-17 – Kaugjuurdepääs: nõuab kaugelt töötavatele mobiilikasutajatele turvalist autentimist ja seansikaitset.

11.4.3 CM-7 – Minimaalne funktsionaalsus: toetab mittevajalike rakenduste ja funktsioonide eemaldamist mobiilsetest lõppseadmetest riski vähendamiseks.

11.4.4 MP-5 – Andmekandjate transpordikaitse: reguleerib andmete turvalist edastamist mobiilsüsteemidest väliste või pilvesihtkohtadeni.

11.4.5 SC-12 – Krüptovõtmete loomine ja vahetamine: nõuab turvaliste krüptograafiliste protokollide kasutamist mobiilses sides ja salvestuses.

11.5 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

11.5.1 Artikkel 5(1)(f) – Terviklus ja konfidentsiaalsus: nõuab organisatsioonidelt isikuandmete kaitsmist mobiilseadmetes loata või õigusvastase juurdepääsu eest.

11.5.2 Artikkel 25 – Lõimitud andmekaitse ja vaikimisi andmekaitse: nõuab andmekaitse lõimimist BYOD- ja MDM-protsessidesse.

11.5.3 Artikkel 32 – Töötlemise turvalisus: nõuab riskipõhiseid kontrollimeetmeid (nt krüptimine, autentimine, juurdepääsukontroll) isikuandmete kaitseks mobiilsetel platvormidel.

11.6 ELi NIS2 direktiiv (2022/2555):

11.6.1 Artikkel 21(2)(d): nõuab, et mobiilne juurdepääs kriitilistele süsteemidele ja teabele oleks kaitstud asjakohaste tehniliste ja korralduslike meetmetega, näiteks lõppseadmete kontrolli, krüptimise ja seirega.

11.7 ELi DORA (2022/2554):

11.7.1 Artikkel 9 – IKT-riski juhtimise raamistik: nõuab finantssektori üksustelt mobiilse ja kaugjuurdepääsu riskide maandamist osana operatsioonilisest toimepidevusest.

11.7.2 Artikkel 10 – IKT-süsteemide turbenõuded: nõuab turvalist mobiilarhitektuuri, seiret ja reageerimismehhanisme mobiilse päritoluga küberohtude jaoks.

11.8 COBIT 2019:

11.8.1 APO13.02 – Infoturbeplaani kehtestamine ja haldamine: nõuab mobiilseadmete kasutuse, sealhulgas BYOD-i, lõimimist organisatsiooni turbestrateegiatesse.

11.8.2 DSS01.04 – Varade konfiguratsiooni ja tervikluse haldamine: kohaldub mobiilseadmete konfiguratsioonikontrollile ja turvalisele juurutamisele.

11.8.3 BAI09.01 – Kontrollimeetmete kehtestamine ja haldamine: toetab tehniliste ja protseduuriliste kaitsemeetmete rakendamist turvaliste mobiilsete ja kaugtoimingute jaoks.