					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P34S					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 regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.1, 5.2, 6.1, 6.2, 8	ISMS-i ning mobiilseadmete ja BYOD-i üldised kontrollinõuded
ISO/IEC 27002:2022	Kontrollimeetmed 5.10–5.13	Üksikasjalikud kontrollimeetmed mobiilseadmete, BYOD-i ja kaugjuurdepääsu jaoks
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Seadmete, andmekandjate ja konfiguratsioonide kontrollimeetmed föderaalses raamistikus
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 5(1)(f)	Isikuandmete ja mobiilsete lõppseadmete kaitse
ELi NIS2 direktiiv	Artikkel 21(2)(d)	Ärikriitiliste seadmete kaitse, sh BYOD
ELi DORA määrus	Artiklid 9, 10	IKT-riski juhtimine ja talitluspidevus mobiilsete lõppseadmete puhul
COBIT 2019	APO13, DSS01, DSS05	IT-juhtimise, operatsioonide ja turvateenuste kontrollimeetmed

1. Eesmärk

1.1. Käesolev poliitika kehtestab kohustuslikud turbenõuded mobiilseadmete, sealhulgas nutitelefonide, tahvelarvutite ja sülearvutite kasutamiseks ettevõtte teabele, süsteemidele või teenustele juurdepääsuks.

1.2. Samuti reguleerib see oma seadme kasutamist tööks (BYOD), et tagada kliendiandmete ja äriandmete kaitse sõltumata seadme omanikust.

1.3. Poliitikaga kehtestatakse ühtsed kaitsemeetmed mobiilsele juurdepääsule, toetatakse ISO/IEC 27001 sertifitseerimise eesmärkide täitmist ning aidatakse vältida andmekadu või kompromiteerimist kadunud, varastatud või väärkasutatud mobiilsete lõppseadmete tõttu.

1.4. Sellega tagatakse, et VKE-des, kus puuduvad spetsiaalsed IT-meeskonnad, rakendatakse mobiilseadmete kasutamisel nii tehnilisi kui ka protseduurilisi kaitsemeetmeid, sealhulgas kaugtöö keskkondades ja pilveteenuste kasutamisel.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile töötajatele, töövõtjatele, praktikantidele ja teenuseosutajatele, kes:

2.1.1. kasutavad mobiilseadet ettevõtte andmetele või süsteemidele juurdepääsuks, nende töötlemiseks või salvestamiseks;

2.1.2. loovad ühenduse ettevõtte teenustega, sealhulgas e-posti, ühiskaustade, pilverakenduste või sisemiste süsteemidega VPN-i kaudu.

2.2. Poliitika hõlmab:

2.2.1. kõiki mobiilseadmeid: nutitelefone, tahvelarvuteid ja sülearvuteid (ettevõtte väljastatud või isiklikud BYOD-seadmed);

2.2.2. kõiki operatsioonisüsteeme (nt iOS, Android, Windows, macOS);

2.2.3. kõiki asukohti (kontor, kodu, kaugtöökoht, avalik ruum).

2.3. Poliitika kehtib kõigis töökeskkondades ning seda tuleb rakendada sõltumata seadme omandivormist.

3. Eesmärgid

3.1. Andmekao vältimine: tagada, et mobiilseadmete kasutamine ei seaks tundlikke ettevõtte- ega kliendiandmeid loata juurdepääsu, varguse ega väärkasutuse ohtu.

3.2. Selgete BYOD-reeglite kehtestamine: määrata jõustatavad tingimused isiklike seadmete kasutamiseks töö eesmärgil ning tagada õiguslikud ja tehnilised kaitsemeetmed.

3.3. Õigusnormidele vastavuse toetamine: täita ISO/IEC 27001, GDPR-i, NIS2 ja muude õiguslike kohustuste nõudeid rakendatavate mobiiliturbe tavade kaudu.

3.4. Tegevusriski vähendamine: vähendada mobiilseadmete väärkasutusest, kompromiteerimisest või rikkest põhjustatud tegevushäirete tõenäosust.

3.5. Klientide usalduse hoidmine: tõendada klientidele ja partneritele, et nende andmed on kaitstud ka siis, kui neile pääsetakse juurde mobiilseadmetest või isiklikest seadmetest.

4. Rollid ja vastutus

4.1. Tegevjuht:

4.1.1. vastutab käesoleva poliitika eest;

4.1.2. kiidab heaks kogu mobiilse juurdepääsu ja BYOD-juurdepääsu ettevõtte süsteemidele;

4.1.3. tagab, et BYOD-kokkulepped on allkirjastatud, säilitatud ja seiratavad;

4.1.4. kontrollib, et välised IT-teenusepakkujad rakendavad nõutud mobiilseadmete kaitsemeetmeid.

4.2. Määratud töötaja või IT-tugi:

4.2.1. toetab tööks kasutatavate mobiilseadmete seadistamist, registreerimist ja konfigureerimist;

4.2.2. rakendab mobiilseadmetega seotud juurdepääsukontrolli, rakenduste piiranguid ja seirepõhimõtteid;

4.2.3. toetab mobiilseadmetega seotud intsidentidele reageerimist (kadunud, varastatud või kompromiteeritud seadmed).

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Iga-aastane läbivaatamine

9.1.1. tegevjuht peab käesoleva poliitika läbi vaatama vähemalt üks kord iga 12 kuu järel.

9.1.2. läbivaatamisel tuleb kontrollida jätkuvat kooskõla ISO/IEC 27001 nõuetega, mobiiltehnoloogiate arenguga ja äritegevuses toimunud muudatustega.

9.1.3. ajakohastamisel tuleb arvesse võtta ka hiljutisi intsidente, audititulemusi ja regulatiivseid arenguid (nt GDPR, NIS2, DORA).

9.2. Vahepealse läbivaatamise aluseks olevad sündmused

9.2.1. käesolevat poliitikat tuleb viivitamata ajakohastada, kui esineb üks järgmistest asjaoludest:

9.2.1.1. oluline mobiiliturbe intsident (nt rikkumine kadunud või häkitud seadme kaudu);

9.2.1.2. muudatus toetatud platvormides või mobiilihalduse tööriistades;

9.2.1.3. õiguslik või regulatiivne muudatus, mis mõjutab isiklike seadmete kasutamist või andmekaitset;

9.2.1.4. uute rakenduste, teenuste või kolmandate osapoolte tööriistade kasutuselevõtt mobiilseadmetes.

9.3. Muudatuste dokumenteerimine

9.3.1. kõik läbivaatamised ja ajakohastamised tuleb dokumenteerida, sealhulgas läbivaatamise kuupäev, tehtud muudatused ja tegevjuhi heakskiit.

9.3.2. auditi eesmärgil tuleb säilitada versioonihalduse ajalugu.

9.4. Teabevahetus ja juurdepääs

9.4.1. tegevjuht peab tagama, et kõik kasutajad (töötajad, töövõtjad, kolmandad osapooled) on muudatustest teavitatud.

9.4.2. uuendatud versioonid peavad olema kergesti kättesaadavad, näiteks ühiskaustades või sisemistel platvormidel.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika on osa VKE infoturbepoliitikate kogumist ja seda tuleb rakendada koos järgmiste poliitikatega:

10.1.1. P4S – Juurdepääsukontrolli poliitika: määratleb nõuded turvalise juurdepääsu haldamiseks süsteemidele, sealhulgas mobiilseadmete kaudu kasutatavatele süsteemidele. Kehtestab paroolihügieeni ja seansikontrolli nõuded.

10.1.2. P8S – Infoturbeteadlikkuse koolituspoliitika: tagab, et kasutajad saavad koolitust mobiilseadmete turvalise kasutamise, intsidentidest teatamise ja BYOD-tingimuste kohta.

10.1.3. P17S – Andmekaitse ja privaatsuspoliitika: kehtestab GDPR-iga kooskõlas oleva isikuandmete ja ettevõtte andmete käitlemise nõuded mobiilsetel platvormidel, eriti siis, kui tööks kasutatakse isiklikke seadmeid.

10.1.4. P9S – Kaugtööpoliitika: ühtlustab mobiilseadmete kasutamise nõuded töö tegemisel väljaspool ettevõtte asukohta või kodust, sealhulgas seadmete käitlemise ja võrgujuurdepääsu kaitsemeetmed.

10.1.5. P30S – Intsidentidele reageerimise poliitika: määrab mobiilseadmetega seotud intsidentide, sealhulgas kompromiteeritud või kadunud seadmete, käsitlemise raamistiku.

10.2. Need seotud poliitikad moodustavad koos tervikliku kontrollimeetmete kogumi mobiilseadmete turbe tagamiseks VKE-des, kus puudub spetsiaalne IT-personal, ning toetavad rakendatavust, läbipaistvust ja sertifitseerimisvalmidust.

11. Viitestandardid ja raamistikud

11.1. Käesolev poliitika toetab täielikku kooskõla järgmiste turbe- ja vastavusstandarditega:

11.2. ISO/IEC 27001:

11.2.1. Punkt 5.1 – Eestvedamine ja pühendumus: tagab juhtkonna järelevalve ja vastutuse mobiilse juurdepääsu ning BYOD-juurdepääsu üle;

11.2.2. Punkt 6.1 – Riskide ja võimaluste käsitlemise meetmed: nõuab mobiiliturbe riskide hindamist ja käsitlemist;

11.2.3. Punkt 8.1 – Tegevuse kavandamine ja ohjamine: nõuab järjepidevaid mobiilse juurdepääsu protseduure äriandmete kaitseks.

11.3. ISO/IEC 27002:

11.3.1. Kontrollimeetmed 5.10 (mobiilseadmete kasutamine), 5.11 (kaugtöö), 5.12 (kaugjuurdepääs) ja 5.13 (BYOD) annavad rakendusjuhised seadmeriskide haldamiseks väikeettevõtte kontekstis.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – mobiilseadmete juurdepääsukontroll: nõuab turvaseadeid autoriseeritud mobiilseks kasutuseks;

11.4.2. AC-20 – väliste süsteemide kasutamine: reguleerib BYOD-i ja kaugjuurdepääsuga seotud riske;

11.4.3. CM-6 – konfiguratsiooniseaded: kehtestab turvalised vaike- ja kohandatud seaded mobiilsetel platvormidel;

11.4.4. MP-7 – andmekandjate kasutamine: käsitleb mobiilsete salvestusvahendite ja andmejuurdepääsu nõuetekohast kasutamist ning piiranguid.

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

11.5.1. Artikkel 5(1)(f) – terviklus ja konfidentsiaalsus: nõuab isikuandmete kaitset asjakohase turvalisuse kaudu, eelkõige mobiilsetel platvormidel;

11.5.2. Artikkel 32 – töötlemise turvalisus: kohustab rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid mobiilseadmetel töödeldavate või salvestatavate andmete kaitseks.

11.6. ELi NIS2 direktiiv (2022/2555):

11.6.1. Artikkel 21(2)(d) – seadmete turvameetmed: nõuab turbekontrolle riist- ja tarkvarale, mida kasutatakse kriitiliste ärisüsteemide kasutamiseks, sealhulgas isiklikes seadmetes.

11.7. ELi DORA määrus (2022/2554):

11.7.1. Artikkel 9 – IKT-riski juhtimise raamistik: nõuab kriitilise tähtsusega ärisuhtluses ja pilveteenustes kasutatavate mobiilsete lõppseadmete kaitset;

11.7.2. Artikkel 10 – IKT talitluspidevus: nõuab turvalise juurdepääsu säilitamist ärisüsteemidele ka häirete või kaugtöö ajal.

11.8. COBIT 2019:

11.8.1. APO13 – turbe juhtimine: nõuab, et organisatsioon rakendaks mobiilseadmete ja BYOD-i poliitikaid kooskõlas ettevõtte riskidega;

11.8.2. DSS01 – operatsioonide juhtimine: tagab turvaliste juurdepääsumehhanismide tehnilise rakendamise;

11.8.3. DSS05 – turvateenuste juhtimine: reguleerib kolmandate osapoolte kaasamist turvaliste mobiilikeskkondade haldamisse ja intsidentidele reageerimise koordineerimisse.