					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P34S					Dokumento pavadinimas: **Mobiliųjų įrenginių ir BYOD politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	5.1, 5.2, 6.1, 6.2, 8 skyriai	Bendrieji ISVS ir mobiliųjų įrenginių / BYOD kontrolės reikalavimai
ISO/IEC 27002:2022	Kontrolės priemonės 5.10–5.13	Išsamios kontrolės priemonės, taikomos mobiliesiems įrenginiams / BYOD ir nuotolinei prieigai
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Federaliniai įrenginių, laikmenų ir konfigūracijos kontrolės reikalavimai
ES BDAR	5 straipsnio 1 dalies f punktas	Asmens duomenų ir mobiliųjų galinių įrenginių apsauga
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	Verslui kritinių įrenginių apsauga, įskaitant BYOD
ES DORA reglamentas	9, 10 straipsniai	IRT rizikos valdymas ir veiklos tęstinumas, taikomi mobiliesiems galiniams įrenginiams
COBIT 2019	APO13, DSS01, DSS05	IT valdysenos, operacijų ir saugumo paslaugų kontrolės priemonės

1. Tikslas

1.1. Ši politika nustato privalomuosius saugumo reikalavimus naudojant mobiliuosius įrenginius, įskaitant išmaniuosius telefonus, planšetinius kompiuterius ir nešiojamuosius kompiuterius, kai jais pasiekiama organizacijos informacija, sistemos ar paslaugos.

1.2. Ji taip pat reglamentuoja nuosavų įrenginių naudojimą (BYOD), siekiant užtikrinti klientų ir verslo duomenų apsaugą, nepriklausomai nuo įrenginio nuosavybės.

1.3. Politika nustato nuoseklias mobiliosios prieigos apsaugos priemones, padeda siekti ISO/IEC 27001 sertifikavimo tikslų ir užkerta kelią duomenų praradimui ar kompromitavimui dėl pamestų, pavogtų ar netinkamai naudojamų mobiliųjų galinių įrenginių.

1.4. Ji užtikrina, kad MVĮ, neturinčiose specializuotų IT komandų, mobiliųjų įrenginių naudojimui būtų taikomos tiek techninės, tiek procedūrinės apsaugos priemonės, įskaitant nuotolinio darbo aplinkas ir debesijos paslaugas.

2. Taikymo sritis

2.1. Ši politika taikoma visiems darbuotojams, rangovams, praktikantams ir paslaugų teikėjams, kurie:

2.1.1. Naudoja mobilųjį įrenginį organizacijos duomenims ar sistemoms pasiekti, tvarkyti arba saugoti

2.1.2. Jungiasi prie organizacijos paslaugų, įskaitant el. paštą, bendrinamus aplankus, debesijos taikomąsias programas ar vidines sistemas, per virtualųjį privatųjį tinklą (VPN)

2.2. Politika apima:

2.2.1. Visus mobiliuosius įrenginius: išmaniuosius telefonus, planšetinius kompiuterius, nešiojamuosius kompiuterius (organizacijos išduotus arba asmeninius BYOD)

2.2.2. Visas operacines sistemas (pvz., iOS, Android, Windows, macOS)

2.2.3. Visas vietas (biurą, namus, nuotolines darbo vietas, viešąsias erdves)

2.3. Politika taikoma visose darbo aplinkose ir turi būti vykdoma nepriklausomai nuo įrenginio nuosavybės.

3. Tikslai

3.1. Užkirsti kelią duomenų praradimui: užtikrinti, kad mobiliųjų įrenginių naudojimas nesudarytų sąlygų jautriems organizacijos ar klientų duomenims tapti prieinamiems dėl neteisėtos prieigos, vagystės ar netinkamo naudojimo.

3.2. Nustatyti aiškias BYOD taisykles: apibrėžti privalomas asmeninių įrenginių naudojimo verslo tikslais sąlygas, užtikrinant teisines ir technines apsaugos priemones.

3.3. Užtikrinti atitiktį reglamentavimo reikalavimams: įgyvendinti ISO/IEC 27001, ES BDAR, NIS2 direktyvos ir kitų teisinių įpareigojimų reikalavimus, taikant privalomąsias mobiliųjų įrenginių saugumo praktikas.

3.4. Mažinti operacinę riziką: sumažinti veiklos sutrikimų tikimybę, kylančią dėl netinkamo mobiliųjų įrenginių naudojimo, kompromitavimo ar veikimo sutrikimų.

3.5. Išlaikyti klientų pasitikėjimą: parodyti klientams ir partneriams, kad jų duomenys išlieka apsaugoti net ir tada, kai jie pasiekiami mobiliaisiais ar asmeniniais įrenginiais.

4. Vaidmenys ir atsakomybės

4.1. Generalinis vadovas (GM):

4.1.1. Atsako už šią politiką.

4.1.2. Tvirtina visą mobiliąją prieigą ir BYOD prieigą prie organizacijos sistemų.

4.1.3. Užtikrina, kad BYOD susitarimai būtų pasirašyti, saugomi ir peržiūrimi.

4.1.4. Patvirtina, kad išorės IT paslaugų teikėjai taiko reikalaujamas mobiliųjų įrenginių apsaugos priemones.

4.2. Paskirtas darbuotojas arba IT pagalbos funkcija:

4.2.1. Padeda atlikti darbui naudojamų mobiliųjų įrenginių parengimą, registravimą ir konfigūravimą.

4.2.2. Įgyvendina su mobiliaisiais įrenginiais susijusias prieigos kontrolės priemones, taikomųjų programų apribojimus ir stebėsenos reikalavimus.

4.2.3. Padeda vykdyti reagavimą į incidentus, susijusius su mobiliaisiais įrenginiais (pamesti, pavogti ar kompromituoti įrenginiai).

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Kasmetinė peržiūra

9.1.1. Generalinis vadovas (GM) privalo peržiūrėti šią politiką bent kartą per 12 mėnesių.

9.1.2. Peržiūros metu turi būti patvirtinama nuolatinė atitiktis ISO/IEC 27001 reikalavimams, besikeičiančioms mobiliųjų technologijų tendencijoms ir verslo operacijų pokyčiams.

9.1.3. Atnaujinant taip pat turi būti atsižvelgiama į naujausius incidentus, audito rezultatus arba reglamentavimo pokyčius (pvz., ES BDAR, NIS2 direktyvą, DORA reglamentą).

9.2. Tarpinės peržiūros inicijavimo įvykiai

9.2.1. Ši politika turi būti nedelsiant atnaujinta, jei įvyksta bent viena iš šių aplinkybių:

9.2.1.1. Esminis mobiliųjų įrenginių saugumo incidentas (pvz., pažeidimas dėl pamesto ar nulaužto įrenginio)

9.2.1.2. Palaikomų platformų arba mobiliųjų įrenginių valdymo priemonių pakeitimas

9.2.1.3. Teisinis arba reglamentavimo pokytis, turintis įtakos asmeninių įrenginių naudojimui arba duomenų apsaugai

9.2.1.4. Naujų taikomųjų programų, paslaugų arba trečiųjų šalių priemonių, naudojamų mobiliuosiuose įrenginiuose, įdiegimas

9.3. Pakeitimų dokumentavimas

9.3.1. Visos peržiūros ir atnaujinimai turi būti dokumentuojami, nurodant peržiūros datą, atliktus pakeitimus ir GM patvirtinimą

9.3.2. Audito tikslais turi būti saugoma versijų valdymo istorija

9.4. Komunikacija ir prieiga

9.4.1. GM turi užtikrinti, kad visi naudotojai (darbuotojai, rangovai, trečiosios šalys) būtų informuoti apie pakeitimus

9.4.2. Atnaujintos versijos turi būti lengvai prieinamos, pavyzdžiui, bendrinamuose aplankuose arba vidinėse platformose

10. Susijusios politikos ir sąsajos

10.1. Ši politika yra bendro MVĮ informacijos saugumo politikų rinkinio dalis ir turi būti įgyvendinama kartu su šiomis politikomis:

10.1.1. P4S – Prieigos kontrolės politika: nustato saugios prieigos prie sistemų valdymo reikalavimus, įskaitant prieigą per mobiliuosius įrenginius. Įtvirtina slaptažodžių higieną ir sesijų kontrolę.

10.1.2. P8S – Informacijos saugumo supratimo ir mokymų politika: užtikrina, kad naudotojai būtų apmokyti saugaus mobiliųjų įrenginių naudojimo, incidentų pranešimo ir BYOD sąlygų klausimais.

10.1.3. P17S – Duomenų apsaugos ir privatumo politika: nustato su ES BDAR suderintą asmens ir organizacijos duomenų tvarkymą mobiliosiose platformose, ypač kai darbui naudojami asmeniniai įrenginiai.

10.1.4. P9S – Nuotolinio darbo politika: suderina mobiliųjų įrenginių naudojimo reikalavimus dirbant ne organizacijos patalpose ar iš namų, įskaitant įrenginių naudojimo ir tinklo prieigos apsaugos priemones.

10.1.5. P30S – Reagavimo į incidentus politika: pateikia reagavimo sistemą mobiliesiems incidentams, įskaitant kompromituotus ar pamestus įrenginius.

10.2. Šios susijusios politikos kartu sudaro visapusišką mobiliųjų įrenginių saugumo kontrolės priemonių rinkinį MVĮ, neturinčioms specializuoto IT personalo, ir užtikrina įgyvendinamumą, skaidrumą bei pasirengimą sertifikavimui.

11. Pamatiniai standartai ir sistemos

11.1. Ši politika padeda užtikrinti visišką atitiktį šiems saugumo ir atitikties standartams:

11.2. ISO/IEC 27001:

11.2.1. 5.1 punktas – Lyderystė ir įsipareigojimas: užtikrina vadovybės priežiūrą ir atskaitomybę už mobiliąją ir BYOD prieigą

11.2.2. 6.1 punktas – Veiksmai rizikoms valdyti: reikalauja vertinti ir tvarkyti mobiliųjų įrenginių saugumo rizikas

11.2.3. 8.1 punktas – Operacinis planavimas ir kontrolė: reikalauja nuoseklių mobiliosios prieigos procedūrų verslo duomenims apsaugoti

11.3. ISO/IEC 27002:

11.3.1. Kontrolės priemonės 5.10 (mobiliųjų įrenginių naudojimas), 5.11 (nuotolinis darbas), 5.12 (nuotolinė prieiga) ir 5.13 (BYOD): pateikia įgyvendinimo gaires, kaip valdyti įrenginių rizikas mažos įmonės kontekste

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – mobiliųjų įrenginių prieigos kontrolė: reikalauja saugumo nuostatų autorizuotam mobiliųjų įrenginių naudojimui

11.4.2. AC-20 – išorės sistemų naudojimas: reglamentuoja BYOD ir nuotolinės prieigos rizikas

11.4.3. CM-6 – konfigūracijos nuostatos: įtvirtina saugius numatytuosius ir pritaikytus nustatymus mobiliosiose platformose

11.4.4. MP-7 – laikmenų naudojimas: apibrėžia tinkamą mobiliųjų laikmenų naudojimą ir prieigos prie duomenų apribojimus

11.5. ES BDAR (2016/679):

11.5.1. 5 straipsnio 1 dalies f punktas – vientisumas ir konfidencialumas: reikalauja užtikrinti duomenų apsaugą, taikant tinkamas asmens duomenų saugumo priemones, ypač mobiliosiose platformose

11.5.2. 32 straipsnis – tvarkymo saugumas: įpareigoja taikyti tinkamas technines ir organizacines priemones duomenims, pasiekiamiems ar saugomiems mobiliuosiuose įrenginiuose, apsaugoti

11.6. ES NIS2 direktyva (2022/2555):

11.6.1. 21 straipsnio 2 dalies d punktas – įrenginių saugumo priemonės: reikalauja taikyti saugumo kontrolės priemones aparatine ir programine įranga, naudojama kritinėms verslo sistemoms pasiekti, įskaitant asmeninius įrenginius

11.7. ES DORA reglamentas (2022/2554):

11.7.1. 9 straipsnis – IRT rizikos valdymo sistema: reikalauja apsaugoti mobiliuosius galinius įrenginius, naudojamus kritinei verslo komunikacijai ir debesijos paslaugoms

11.7.2. 10 straipsnis – IRT veiklos tęstinumas: reikalauja užtikrinti nuolatinę saugią prieigą prie verslo sistemų net sutrikimų ar nuotolinio darbo metu

11.8. COBIT 2019:

11.8.1. APO13 – saugumo valdymas: reikalauja, kad organizacija taikytų mobiliųjų įrenginių ir BYOD politiką, suderintą su įmonės rizika

11.8.2. DSS01 – operacijų valdymas: užtikrina techninį saugios prieigos mechanizmų įgyvendinimą

11.8.3. DSS05 – saugumo paslaugų valdymas: reglamentuoja trečiųjų šalių dalyvavimą palaikant saugias mobiliąsias aplinkas ir koordinuojant reagavimą į incidentus