					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P34					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	Punktas / straipsnis	Pastaba
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Taikomos saugumo kontrolės priemonės ir atitikties reikalavimai
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Nustatomos išsamios mobiliųjų įrenginių valdymo kontrolės priemonės
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Prieigos kontrolė, nuotolinė prieiga, konfigūravimo ir saugumo reikalavimai mobiliesiems įrenginiams
ES BDAR	5 straipsnio 1 dalies f punktas, 25, 32	Privalomi privatumo, duomenų šifravimo ir tvarkymo saugumo reikalavimai
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	Mobiliajai prieigai taikomos techninės ir organizacinės apsaugos priemonės
ES DORA reglamentas	9, 10	IRT rizikos valdymo ir mobiliųjų įrenginių saugumo reikalavimai
COBIT 2019	APO13.02, DSS01.04, BAI09	Informacijos saugumo planai, turto konfigūravimas ir mobiliųjų aplinkų kontrolės priemonės

1. Tikslas

1.1 Ši politika nustato saugumo, atitikties ir eksploatacinius reikalavimus mobiliųjų įrenginių ir asmeninių technologijų naudojimui (nuosavų įrenginių naudojimas (BYOD)), kai jais jungiamasi prie organizacijos sistemų, taikomųjų programų ar duomenų.

1.2 Ja siekiama užtikrinti bendrovės informacijos, pasiekiamos ar tvarkomos per mobiliuosius galinius įrenginius, konfidencialumą, vientisumą ir prieinamumą, įskaitant išmaniuosius telefonus, planšetinius kompiuterius, nešiojamuosius kompiuterius ir hibridinius įrenginius.

1.3 Ši politika taip pat nustato technines ir procedūrines kontrolės priemones, būtinas mažinti tokias rizikas kaip duomenų nutekėjimas, neteisėta prieiga, įrenginio praradimas ar vagystė ir mobiliųjų taikomųjų programų kompromitavimas.

1.4 Ši politika padeda užtikrinti atitiktį reglamentavimo ir sutartiniams reikalavimams, kartu sudarydama sąlygas saugiam mobiliam darbui darbuotojams, rangovams ir įgaliotoms trečiosioms šalims.

2. Taikymo sritis

2.1 Ši politika taikoma visam personalui, įskaitant darbuotojus, rangovus, praktikantus ir trečiųjų šalių paslaugų teikėjus, kurie naudoja mobiliuosius įrenginius prieigai prie bendrovės duomenų, sistemų, taikomųjų programų ar komunikacijos platformų gauti.

2.2 Ji apima visus mobiliojo skaičiavimo įrenginius, įskaitant, bet neapsiribojant:

2.2.1 išmaniaisiais telefonais ir planšetiniais kompiuteriais (iOS, Android ir kt.)

2.2.2 nešiojamaisiais kompiuteriais ir ultrabook tipo įrenginiais (Windows, macOS, Linux)

2.2.3 dėvimais įrenginiais ir hibridiniais išmaniaisiais įrenginiais, galinčiais sinchronizuoti duomenis

2.3 Ji taikoma nepriklausomai nuo to, ar įrenginys priklauso bendrovei, ar yra asmeninis ir naudojamas pagal BYOD susitarimą.

2.4 Politika apima visus prieigos kanalus, įskaitant VPN, virtualiuosius darbalaukius, debesijos taikomąsias programas, el. paštą, bendradarbiavimo platformas (pvz., SharePoint, Teams) ir failų sinchronizavimo priemones (pvz., OneDrive, Dropbox, jei jos yra autorizuotos).

2.5 Ji taikoma dirbant nuotoliniu būdu, vietinėje infrastruktūroje, kelionėse ar taikant hibridinio darbo modelį.

3. Tikslai

3.1 Mažinti duomenų kompromitavimo, nutekėjimo ar praradimo riziką dėl nesaugaus mobiliųjų įrenginių naudojimo.

3.2 Užtikrinti nuoseklų ir privalomą saugumo kontrolės priemonių taikymą visuose mobiliuosiuose galiniuose įrenginiuose, nepriklausomai nuo jų nuosavybės modelio (organizacijos ar BYOD).

3.3 Užtikrinti, kad mobiliųjų įrenginių naudojimas atitiktų ISO/IEC 27001 ir kitus duomenų privatumo, apsaugos ir kibernetinio saugumo srityse taikomus reguliavimo pagrindus.

3.4 Sudaryti sąlygas saugiai integruoti mobiliuosius įrenginius į organizacijos veiklos, komunikacijos ir bendradarbiavimo procesus.

3.5 Nustatyti aiškias atsakomybes ir procesus mobiliųjų įrenginių valdymui (MDM), įskaitant įtraukimą, nuotolinį ištrynimą, šifravimą, autentifikavimą ir stebėseną.

3.6 Apsaugoti asmenų, naudojančių savo įrenginius, privatumo teises kartu užtikrinant organizacijos jautrių duomenų apsaugą.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO) / IT saugumo vadovas

4.1.1 Nustato politiką ir techninius standartus mobiliųjų įrenginių ir BYOD naudojimui.

4.1.2 Vykdo mobiliųjų įrenginių kontrolės priemonių atitikties, reagavimo į incidentus ir išimčių valdymo priežiūrą.

4.1.3 Koordinuoja veiksmus su teisinės ir žmogiškųjų išteklių funkcijų atstovais, kad politikos taikymas būtų teisiškai pagrįstas ir suderintas su organizacijos praktika.

4.2 Informacinių technologijų (IT) administratorius / MDM administratorius

4.2.1 Valdo mobiliųjų įrenginių naudotojų prieigos suteikimą, įtraukimą ir konfigūravimą per MDM sprendimus.

4.2.2 Taiko įrenginio lygmens kontrolės priemones (pvz., šifravimą, PIN kodus, taikomųjų programų kontrolę).

4.2.3 Atlieka nuotolinį ištrynimą, įrenginio užrakinimą ir prieigos teisių atšaukimą, kai to reikia.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Šią politiką ne rečiau kaip kartą per metus turi peržiūrėti informacijos saugumo vadovas (CISO) arba paskirtas informacijos saugumo vadovas, siekdamas užtikrinti suderinamumą su:

9.1.1 mobiliųjų operacinių sistemų platformų, MDM technologijų ar autentifikavimo standartų pokyčiais;

9.1.2 reguliavimo ar sutartiniais pokyčiais, darančiais poveikį mobiliųjų duomenų apsaugai (pvz., ES BDAR, DORA reglamentas, NIS2 direktyva);

9.1.3 ISO/IEC 27001:2022, ISO/IEC 27002:2022 ar NIST SP 800-53 Rev.5 kontrolės rinkinių pakeitimais;

9.1.4 auditų, paskesniųjų incidentų peržiūrų ar darbuotojų grįžtamuoju ryšiu.

9.2 Tarpinės peržiūros gali būti inicijuojamos dėl:

9.2.1 saugumo incidentų, susijusių su mobiliaisiais įrenginiais ar BYOD platformomis;

9.2.2 tiekėjo pranešimo apie didelės rizikos pažeidžiamumus palaikomose platformose;

9.2.3 naujų mobiliųjų taikomųjų programų ar bendradarbiavimo platformų, naudojamų veiklos procesuose, įdiegimo.

9.3 Politikos atnaujinimai turi būti:

9.3.1 dokumentuojami politikos versijų istorijoje;

9.3.2 komunikuojami visam personalui ir paveiktiems rangovams;

9.3.3 pakartotinai patvirtinami, atnaujinant patvirtinimą visiems BYOD naudotojams.

9.4 Visos peržiūros ir pakeitimai turi būti formaliai patvirtinti vadovybės ir užregistruoti politikos pakeitimų registre.

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra susijusi su keliomis svarbiomis organizacijos ISVS politikomis. Pagrindinės sąsajos:

10.1.1 P1 – Informacijos saugumo politika: nustato bendruosius valdysenos principus visoms informacijos saugumo kontrolės priemonėms, įskaitant mobiliųjų įrenginių naudojimo kontrolę.

10.1.2 P3 – Priimtino naudojimo politika: apibrėžia leidžiamą elgseną ir apribojimus, susijusius su technologijų naudojimu, kurie tiesiogiai taikomi mobiliajai ir BYOD prieigai.

10.1.3 P9 – Nuotolinio darbo politika: nustato papildomus saugumo reikalavimus mobilioms darbo aplinkoms ir papildo šioje politikoje nustatytas mobiliesiems įrenginiams skirtas kontrolės priemones.

10.1.4 P13 – Duomenų klasifikavimo ir ženklinimo politika: nustato, kaip duomenys mobiliuosiuose įrenginiuose turi būti tvarkomi pagal klasifikavimo lygį, o tai daro poveikį saugojimui, perdavimui ir šifravimo taikymui.

10.1.5 P22 – Žurnalų tvarkymo ir stebėsenos politika: palaiko mobiliosios prieigos žurnalų rinkimą ir peržiūrą anomalijoms ar pažeidimams nustatyti.

10.1.6 P30 – Reagavimo į incidentus politika: nustato, kaip tvarkomi ir eskaluojami su mobiliaisiais įrenginiais susiję incidentai (pvz., įrenginio praradimas, neteisėta prieiga).

10.1.7 P33 – Audito ir atitikties stebėsenos politika: nustato pagrindą periodiniams mobiliojo saugumo atitikties patikrinimams, įskaitant BYOD politikos laikymąsi.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintais kibernetinio saugumo pagrindais ir teisiniais įpareigojimais, siekiant užtikrinti saugų mobiliųjų įrenginių ir asmeninių (BYOD) technologijų naudojimą organizacijos aplinkoje.

11.2 ISO/IEC 27001:

11.2.1 5.10 punktas – informacijos ir turto priimtinas naudojimas: reikalauja taikyti kontrolės priemones atsakingam organizacijos turto naudojimui, įskaitant mobiliuosius įrenginius.

11.2.2 5.11 punktas – nuotolinis darbas: reglamentuoja saugią praktiką jungiantis prie sistemų už bendrovės patalpų ribų.

11.2.3 5.12 punktas – mobiliųjų įrenginių naudojimas: nustato pareigą taikyti rizika grindžiamas kontrolės priemones mobiliesiems galiniams įrenginiams ir BYOD konfigūracijoms.

11.2.4 5.13 punktas – informacijos perdavimas: nustato perduodamos informacijos apsaugos per mobiliuosius kanalus reikalavimus.

11.3 ISO/IEC 27002:2022 – 5.10–5.13 kontrolės priemonės:

11.3.1 A priedo 5.10–5.13 kontrolės priemonės nurodo, kaip ISVS turi būti taikoma mobilioji prieiga, šifravimas, stebėsena ir praradimo rizikos mažinimas. Šios kontrolės priemonės pateikia išsamias įgyvendinimo gaires, kaip apsaugoti mobiliuosius galinius įrenginius, taikyti konteinerizaciją, stebėti įrenginio vientisumą ir užtikrinti į privatumo apsaugą orientuotas BYOD konfigūracijas.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – prieigos kontrolė mobiliesiems įrenginiams: apibrėžia bazines apsaugos priemones, įskaitant šifravimą, autentifikavimą ir MDM taikymą.

11.4.2 AC-17 – nuotolinė prieiga: reikalauja saugaus autentifikavimo ir sesijų apsaugos nuotoliniams mobiliųjų įrenginių naudotojams.

11.4.3 CM-7 – mažiausio funkcionalumo principas: numato nereikalingų taikomųjų programų ir funkcijų pašalinimą iš mobiliųjų galinių įrenginių rizikai mažinti.

11.4.4 MP-5 – laikmenų transportavimo apsauga: reglamentuoja saugų duomenų perdavimą iš mobiliųjų sistemų į išorines ar debesijos paskirtis.

11.4.5 SC-12 – kriptografinių raktų generavimas: nustato pareigą naudoti saugius kriptografinius protokolus mobiliajam ryšiui ir duomenų saugojimui.

11.5 ES BDAR (2016/679):

11.5.1 5 straipsnio 1 dalies f punktas – vientisumas ir konfidencialumas: reikalauja, kad organizacijos apsaugotų asmens duomenis mobiliuosiuose įrenginiuose nuo neteisėtos prieigos.

11.5.2 25 straipsnis – duomenų apsauga pagal projektavimą ir pagal numatytuosius nustatymus: reikalauja privatumo apsaugą integruoti į BYOD ir MDM procesus.

11.5.3 32 straipsnis – tvarkymo saugumas: nustato rizika grindžiamas kontrolės priemones (pvz., šifravimą, autentifikavimą, prieigos kontrolę) asmens duomenims mobiliosiose platformose.

11.6 ES NIS2 direktyva (2022/2555):

11.6.1 21 straipsnio 2 dalies d punktas: nustato, kad mobilioji prieiga prie kritinių sistemų ir informacijos turi būti apsaugota taikant tinkamas technines ir organizacines priemones, tokias kaip galinių įrenginių kontrolė, šifravimas ir stebėsena.

11.7 ES DORA reglamentas (2022/2554):

11.7.1 9 straipsnis – IRT rizikos valdymo sistema: reikalauja, kad finansų sektoriaus subjektai mažintų mobiliųjų įrenginių ir nuotolinės prieigos riziką kaip operacinio atsparumo dalį.

11.7.2 10 straipsnis – IRT sistemų saugumo reikalavimai: nustato saugios mobiliųjų įrenginių architektūros, stebėsenos ir reagavimo mechanizmų reikalavimus dėl per mobiliuosius įrenginius kylančių kibernetinių grėsmių.

11.8 COBIT 2019:

11.8.1 APO13.02 – informacijos saugumo plano nustatymas ir palaikymas: reikalauja, kad mobiliųjų įrenginių naudojimas, įskaitant BYOD, būtų integruotas į organizacijos saugumo strategiją.

11.8.2 DSS01.04 – turto konfigūracijos ir vientisumo valdymas: taikoma mobiliųjų įrenginių konfigūracijos kontrolei ir saugiam diegimui.

11.8.3 BAI09.01 – kontrolės priemonių nustatymas ir palaikymas: palaiko techninių ir procedūrinių apsaugos priemonių įgyvendinimą saugioms mobilioms ir nuotolinėms operacijoms.