					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P03					Dokumento pavadinimas: **Priimtino naudojimo 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**

Suderinamumas su taikomais standartais ir reglamentavimo reikalavimais

Standartas / reglamentavimas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5 skyrius	Nustato elgsenos normas ir reikalavimus priimtino naudojimo politikai
ISO/IEC 27002:2022	6.1, 6.2, 8.1, 8.12 kontrolės priemonės	Pateikia gaires dėl informacijos saugumo atsakomybių, informuotumo, taip pat įrenginių ir duomenų valdysenos
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Prieigos valdymo ir informuotumo / elgsenos kontrolės priemonės, susijusios su IT turto naudojimu
ES BDAR	5 straipsnio 1 dalies f punktas, 32 straipsnis; 39 konstatuojamoji dalis	Įtvirtina konfidencialumo ir vientisumo užtikrinimą, nustato techninių ir organizacinių priemonių reikalavimą bei teisinius tinkamo naudojimo pagrindus
ES NIS2 direktyva	21 straipsnio 2 dalies a–d punktai	Nustato veiklos politikų ir saugaus naudojimo mokymų reikalavimus
ES DORA reglamentas	5 straipsnis	Palaiko IRT rizikos valdymą, reglamentuodamas naudotojų elgseną
COBIT 2019	APO07, BAI05, DSS05, MEA01	Žmogiškųjų išteklių, pokyčių valdymo, valdomo saugumo, atitikties ir veiklos stebėsenos sritys

1. Tikslas

1.1 Ši politika nustato priimtiną ir nepriimtiną organizacijos informacinių sistemų, kompiuterinių išteklių, ryšių priemonių ir duomenų tvarkymo praktikos naudojimą.

1.2 Ji užtikrina, kad visi naudotojai suprastų savo atsakomybes naudodamiesi įmonės IT turtu ir kad jų veiksmai palaikytų informacijos konfidencialumą, vientisumą, prieinamumą ir teisėtą tvarkymą.

1.3 Ši politika įgyvendina ISO/IEC 27001:2022 5.10 punkto reikalavimą, nustatydama sistemų naudojimo elgsenos normas ir taikydama technines bei procedūrines apsaugos priemones, siekiant sumažinti netinkamo naudojimo, aplaidumo ar piktnaudžiavimo riziką.

1.4 Ji taip pat palaiko tyrimo ir politikos vykdymo užtikrinimo veiklas, įskaitant reagavimą į incidentus ir drausminių priemonių taikymą pažeidimų atvejais.

2. Taikymo sritis

2.1 Ši politika taikoma visiems asmenims ir subjektams, kuriems suteikta prieiga prie organizacijos informacinių sistemų ir turto, įskaitant, bet tuo neapsiribojant:

2.1.1 darbuotojus, rangovus, konsultantus, praktikantus ir laikinųjų darbuotojų agentūrų personalą;

2.1.2 trečiųjų šalių tiekėjus, turinčius prieigą prie sistemų arba deleguotus administratoriaus vaidmenis;

2.1.3 svečius ar partnerius, naudojančius organizacijai priklausančią arba patvirtintą IT infrastruktūrą.

2.2 Taikymo sritis apima visą organizacijos technologinį ir duomenų turtą, įskaitant:

2.2.1 darbo vietų kompiuterius, nešiojamuosius kompiuterius, mobiliuosius įrenginius ir serverius;

2.2.2 tinklo infrastruktūrą ir debesijos paslaugas;

2.2.3 el. paštą, žinučių siuntimo sistemas, bylų saugyklas, bendradarbiavimo platformas ir VPN;

2.2.4 saugomus, perduodamus ar tvarkomus duomenis, nepriklausomai nuo jų formato ar vietos;

2.2.5 bet kurį asmeninį įrenginį, naudojamą pagal BYOD (Bring Your Own Device) modelį ir prijungiamą prie organizacijos sistemų.

2.3 Ši politika taikoma visose darbo aplinkose, įskaitant:

2.3.1 įmonės biurus ir gamybos vietas;

2.3.2 nuotolinio darbo vietas ar hibridinio darbo modelius;

2.3.3 veiklą lauko sąlygomis arba trečiųjų šalių valdomose patalpose.

2.4 Visi naudotojai, kaip prieigos prie įmonės sistemų ar įmonės duomenų tvarkymo sąlygą, privalo patvirtinti susipažinimą su šia politika ir jos laikytis.

3. Tikslai

3.1 Nustatyti ir taikyti organizacijos IT išteklių priimtino naudojimo taisykles.

3.2 Užkirsti kelią neteisėtai prieigai, duomenų nutekėjimui ar žalai, atsirandančiai dėl neatsargaus ar piktavališko naudojimo.

3.3 Apsaugoti įmonės tinklus, turtą ir duomenis nuo grėsmių, kylančių dėl naudotojų elgsenos.

3.4 Užtikrinti teisinių ir sutartinių įsipareigojimų vykdymą, demonstruojant deramą rūpestingumą IT išteklių valdysenoje.

3.5 Užtikrinti nuoseklumą ir aiškumą taikant drausminių priemonių ir išimčių valdymo procesus.

3.6 Skatinti etiško, saugaus ir atsakingo skaitmeninių ir fizinių kompiuterinių išteklių naudojimo kultūrą.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina priimtino naudojimo politiką (AUP) ir užtikrina, kad ji būtų suderinta su verslo tikslais, reglamentavimo reikalavimais ir organizacijos vertybėmis.

4.1.2 Skiria išteklius politikos įgyvendinimui, mokymams, stebėsenai ir politikos peržiūrai.

4.1.3 Kaip ISVS valdysenos dalis peržiūri atitikties būklę ir drausmines priemones, susijusias su politikos pažeidimais.

4.2 IT ir informacijos saugumo komandos

4.2.1 Įgyvendina technines apsaugos priemones šios politikos reikalavimams užtikrinti, įskaitant:

4.2.2 turinio filtravimo, apsaugos nuo kenkimo programinės įrangos, galinių įrenginių saugos ir tinklo stebėsenos priemones;

4.2.3 el. pašto saugos konfigūracijas ir duomenų praradimo prevencijos (DLP) sprendimus;

4.2.4 draudžiamųjų ir leidžiamųjų sąrašų taikymą programinei įrangai, aparatinei įrangai ir interneto svetainėms.

4.2.5 Tvarko patvirtintos ir draudžiamos programinės įrangos, įrenginių ir paslaugų inventorių.

4.2.6 Tiria įtariamus AUP pažeidimus, renka skaitmeninės kriminalistikos įrodymus ir, kai tikslinga, palaiko drausminių ar teisinių priemonių taikymą.

4.2.7 Bendradarbiauja su Žmogiškųjų išteklių ir Teisės padaliniais valdant incidentus, juos eskaluojant ir vykdant pranešimo pareigas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Peržiūros pagrindai ir dažnumas

9.1.1 Ši politika turi būti peržiūrima:

9.1.1.1 ne rečiau kaip kartą per metus;

9.1.1.2 po bet kokių reikšmingų technologijų ar infrastruktūros pokyčių;

9.1.1.3 po incidentų ar audito išvadų, atskleidusių politikos taikymo spragas;

9.1.1.4 pasikeitus taikomiems teisės aktams ar sutartiniams reikalavimams.

9.2 Atsakomybė ir tvirtinimas

9.2.1 Už peržiūros procesą atsako CISO arba paskirtas ISVS vadovas.

9.2.2 Atnaujinimai turi būti patvirtinti vadovybės ir komunikuoti visai organizacijai.

9.2.3 Pakartotinai išleidus politiką, atnaujintų nuostatų patvirtinimas turi būti surinktas iš naujo.

9.3 Dokumentų valdymas

9.3.1 Politikoje turi būti nurodyti šie metaduomenys ir versijavimo duomenys:

9.3.1.1 pavadinimas, identifikatorius ir klasifikavimo lygis;

9.3.1.2 politikos savininkas ir dokumento administratorius;

9.3.1.3 pakeitimų istorija ir atnaujinimų pagrindimas;

9.3.1.4 peržiūros data ir kitos planinės peržiūros data;

9.3.1.5 platinimo ir patvirtinimo žurnalo nuorodos.

9.3.2 Pagrindinė kopija turi būti saugoma ISVS dokumentų saugykloje, taikant versijų kontrolę.

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti aiškinama kartu su šiomis politikomis:

10.1.1 P1 – Informacijos saugumo politika: nustato pagrindinius elgsenos lūkesčius ir aukščiausio lygio vadovybės įsipareigojimą dėl priimtino naudojimo.

10.1.2 P4 – Prieigos valdymo politika: apibrėžia leidimus ir teises, susijusias su naudotojų, sistemų ir duomenų prieiga, ir tiesiogiai užtikrina priimtino naudojimo ribas.

10.1.3 P6 – Rizikos valdymo politika: apima su elgsena susijusias rizikas ir palaiko stebėsenos bei rizikos mažinimo veiklas, susijusias su naudotojų sukeltomis grėsmėmis.

10.1.4 P7 – Įdarbinimo ir darbo santykių nutraukimo politika: užtikrina, kad priimtino naudojimo sąlygos būtų patvirtinamos darbo pradžioje ir panaikinamos darbo santykiams pasibaigus.

10.1.5 P9 – Nuotolinio darbo politika: išplečia priimtino naudojimo nuostatas nuotolinio ir hibridinio darbo aplinkoms.

10.2 Šios susijusios politikos sudaro sluoksniuotosios gynybos modelį elgsenos, techninės ir sutartinės valdysenos srityse.

11. Pamatiniai standartai ir sistemos

11.1 Ši priimtino naudojimo politika (AUP) yra suderinta su tarptautiniu mastu pripažintais standartais ir teisinėmis sistemomis, siekiant užtikrinti taikytinas, audituojamas ir rizika grindžiamas elgsenos kontrolės priemones visame skaitmeninių ir fizinių informacinių sistemų naudojime.

11.2 ISO/IEC 27001:2022

11.2.1 5.10 punktas – informacijos ir kito susijusio turto priimtinas naudojimas: ši politika tiesiogiai įgyvendina reikalavimą apibrėžti, komunikuoti ir taikyti taisykles, reglamentuojančias tinkamą IT išteklių naudojimą.

11.2.2 A priedo 6.1 kontrolės priemonė – atsakomybė už informacijos saugumą: nustato aiškias atsakomybes dėl naudotojų elgsenos ir atitikties priežiūros.

11.2.3 A priedo 6.2 kontrolės priemonė – informacijos saugumo žinomumas, švietimas ir mokymas: į AUP taikymą įtraukiami mokymai ir politikos patvirtinimo procesai.

11.2.4 A priedo 8.1 kontrolės priemonė – naudotojų galiniai įrenginiai ir 8.12 kontrolės priemonė – duomenų praradimo prevencija: apima priimtiną elgseną naudotojų įrenginiuose ir reglamentuoja veiklas, galinčias lemti duomenų atskleidimą ar nutekėjimą.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (prieigos valdymas mobiliuosiuose įrenginiuose) ir AC-20 (išorinių informacinių sistemų naudojimas): ši politika nustato naudotojų pareigas ir apribojimus BYOD ir trečiųjų šalių sistemų prieigos atvejais.

11.3.2 PL-4 (elgsenos taisyklės): pateikia išsamius priimtino naudojimo reikalavimus, atitinkančius šią politiką.

11.3.3 AT-2 (saugumo informuotumo mokymai): įgyvendinama per naudotojų mokymus ir dokumentuotą politikos patvirtinimą.

11.3.4 AU-2 (audituojami įvykiai) ir AU-12 (audito generavimas): politikos vykdymo užtikrinimas remiasi naudotojų veiksmų stebėsena ir perspėjimais apie pažeidimus.

11.4 ES BDAR (2016/679):

11.4.1 5 straipsnio 1 dalies f punktas: įtvirtina asmens duomenų saugumą ir vientisumą; ši politika mažina dėl žmonių elgsenos ir neteisėto naudojimo kylančias rizikas.

11.4.2 32 straipsnis: nustato techninių ir organizacinių priemonių, tokių kaip elgsenos kontrolės priemonės ir naudojimo apribojimai, reikalavimą asmens duomenims apsaugoti.

11.4.3 39 konstatuojamoji dalis: pabrėžia būtinybę užtikrinti, kad tik įgalioti asmenys turėtų tik būtiną prieigą ir teisėtai naudotų duomenis.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies a–d punktai: reikalauja veiklos politikų ir mokymų saugiam sistemų naudojimui; ši AUP tai įgyvendina apibrėždama elgseną, stebėseną ir politikos vykdymo užtikrinimo procesus.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 5 straipsnis: ši politika palaiko IRT rizikos valdymo sistemą, nustatydama žmogaus ir sistemos sąveikos taisykles ir mažindama su elgsena susijusią kibernetinę riziką.

11.7 COBIT 2019:

11.7.1 APO07 – valdomi žmogiškieji ištekliai: užtikrina naudotojų atsakomybes ir informuotumą viso darbuotojo ciklo metu.

11.7.2 BAI05 – valdomi organizaciniai pokyčiai: integruoja priimtino naudojimo valdyseną į pokyčių procesus, darančius įtaką naudotojų elgsenai.

11.7.3 DSS05 – valdomos saugumo paslaugos: palaiko naudotojų veiklos stebėseną, elgsenos perspėjimus ir automatizuotus reagavimo mechanizmus.

11.7.4 MEA01 – stebėti, vertinti ir analizuoti veiklą bei atitiktį: politika nustato rodiklius ir mechanizmus, skirtus patvirtinti naudotojų atitiktį elgsenos lūkesčiams.