					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P08					Dokumento pavadinimas: **Informacijos saugumo supratimo ir mokymo 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	7.3 skyrius, A priedo kontrolė 6.3	Nustato informuotumo ir mokymų reikalavimus, kuriuos apima ši politika
ISO/IEC 27002:2022	Kontrolė 6	Palaiko tinkamus, pagal pareigas pritaikytus informuotumo mokymus
NIST SP 800-53 Rev.5	AT-1–AT-5	Suderinta su politikomis ir procedūromis, informuotumo mokymais, vaidmenimis grindžiamais mokymais, mokymų įrašais ir ryšiu su saugumo grupėmis
ES BDAR	32, 39 straipsniai; 78 konstatuojamoji dalis	Nustato mokymų reikalavimą asmens duomenų tvarkytojams ir bendrą darbuotojų informuotumą
ES NIS2 direktyva	21(2)(a, b), 21(3) straipsniai	Reikalauja rizikos ir saugumo mokymų politikų bei informuotumo iniciatyvų
ES DORA reglamentas	5, 8, 13 straipsniai	Reikalauja IRT rizikos informuotumo ir mokymų kaip atsparumo kontrolės priemonių dalies
COBIT 2019	APO07, DSS05, MEA	Stiprina darbuotojų informuotumą, naudotojų švietimą ir atitikties stebėseną

1. Tikslas

1.1 Ši politika nustato oficialią sistemą, skirtą užtikrinti, kad visas personalas būtų supažindintas su savo informacijos saugumo atsakomybėmis ir gautų mokymus, būtinus informacijos išteklių konfidencialumui, vientisumui ir prieinamumui apsaugoti.

1.2 Ji įgyvendina ISO/IEC 27001 7.3 skyriaus ir A priedo kontrolės 6.3 reikalavimus, nustatydama struktūrizuotą ir rizika grindžiamą informuotumo didinimo ir mokymo programą, pritaikytą organizaciniams vaidmenims ir kintančioms grėsmėms.

1.3 Ši politika padeda mažinti su žmonėmis susijusius pažeidžiamumus, skatinti saugų elgesį ir nuosekliai stiprinti saugias praktikas pagal reglamentavimo ir sutartinius reikalavimus.

2. Taikymo sritis

2.1 Ši politika taikoma visiems vidiniams ir išoriniams asmenims, turintiems prieigą prie organizacijos informacinių sistemų, duomenų ar patalpų, įskaitant:

2.1.1 darbuotojus (dirbančius visą darbo laiką, ne visą darbo laiką ir laikinus darbuotojus);

2.1.2 rangovus, konsultantus, tiekėjus ir praktikantus;

2.1.3 trečiąsias šalis, turinčias loginę arba fizinę prieigą pagal paslaugų sutartis.

2.2 Taikymo sritis apima:

2.2.1 įvadinius saugumo informuotumo mokymus;

2.2.2 konkretiems vaidmenims skirtus mokymus (pvz., programuotojams, finansų darbuotojams, privilegijuotiesiems naudotojams);

2.2.3 periodinius pakartotinius mokymus ir informuotumo kampanijas;

2.2.4 ad hoc mokymus reaguojant į incidentus ar naujas grėsmes.

2.3 Šios politikos apimami mokymų teikimo mechanizmai apima e. mokymą, kontaktinius instruktažus, simuliacijas, žinių patikrinimus, plakatus, naujienlaiškius ir privalomus patvirtinimus.

3. Tikslai

3.1 Užtikrinti, kad visas personalas suprastų savo atsakomybes saugant organizacijos turtą ir laikantis saugumo politikų.

3.2 Teikti nuolatinius, išmatuojamus informuotumo mokymus, suderintus su vaidmenimis grindžiama rizikos ekspozicija.

3.3 Įtvirtinti saugų elgesį kasdienėje veikloje, stiprinant tokias praktikas kaip saugus slaptažodžių naudojimas, pranešimas apie incidentus ir atsparumas fišingui.

3.4 Užtikrinti atitiktį reglamentavimo reikalavimams ir pasirengimą auditui, susijusį su informacijos saugumo mokymų reikalavimais įvairiose pramonės šakose ir jurisdikcijose.

3.5 Mažinti saugumo incidentus, kylančius dėl neatsargumo, informuotumo stokos ar netinkamo sprendimo, pasitelkiant elgsenos formavimą ir nuolatinį stiprinimą.

4. Vaidmenys ir atsakomybės

4.1 Vykdomoji vadovybė

4.1.1 Tvirtina organizacijos informacijos saugumo mokymų strategiją ir užtikrina, kad jai būtų skirti reikiami ištekliai ir ji būtų integruota į organizacijos prioritetus.

4.1.2 Vadovybės lygmeniu stebi atitiktį ir užtikrina politikos laikymąsi visuose padaliniuose.

4.2 Vyriausiasis informacijos saugumo pareigūnas / ISVS vadovas

4.2.1 Atsako už šią politiką ir apibrėžia informuotumo ir mokymų sistemą pagal riziką, atitiktį ir verslo poreikius.

4.2.2 Prižiūri visų saugumo mokymų iniciatyvų projektavimą, teikimą, stebėseną ir peržiūrą.

4.2.3 Užtikrina, kad mokymai būtų periodiškai atnaujinami ir atspindėtų kintančias grėsmes bei naujas technologijas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Peržiūros dažnumas

9.1.1 Ši politika ir susijusi mokymų programa turi būti peržiūrimos:

9.1.1.1 kasmet; arba

9.1.1.2 po didelių incidentų, susijusių su žmogiškąja klaida arba vidine grėsme;

9.1.1.3 diegiant reikšmingas naujas technologijas arba atsiradus naujoms grėsmėms;

9.1.1.4 pasikeitus teisiniams, sutartiniams arba sertifikavimo įpareigojimams.

9.2 Peržiūros procesas

9.2.1 Peržiūrai turi vadovauti vyriausiasis informacijos saugumo pareigūnas, koordinuodamas veiksmus su:

9.2.1.1 žmogiškųjų išteklių ir mokymų padaliniais;

9.2.1.2 teisininkais ir duomenų apsaugos pareigūnais;

9.2.1.3 IT saugumo ir operacinės rizikos funkcijomis.

9.2.2 Visi atnaujinimai turi būti:

9.2.2.1 patvirtinti Informacijos saugumo valdymo komiteto;

9.2.2.2 valdomi pagal versijų kontrolę ir dokumentuojami ISVS dokumentų registre;

9.2.2.3 perduodami naudotojams, jei esminiai pokyčiai daro poveikį mokymų taikymo sričiai arba atsakomybėms.

9.3 Turinio atnaujinimo valdysena

9.3.1 Mokymų moduliai ir informuotumo medžiaga turi būti peržiūrimi kas 12 mėnesių, siekiant užtikrinti:

9.3.1.1 aktualumą grėsmių aplinkai;

9.3.1.2 reglamentavimo tikslumą;

9.3.1.3 formato suderinamumą (pvz., prieinamumą, lokalizavimą).

9.3.2 Pasenęs arba klaidinantis turinys turi būti nedelsiant pašalintas ir pakeistas patvirtintomis alternatyvomis.

10. Susijusios politikos ir sąsajos

10.1 Ši politika yra palaikoma toliau nurodytų politikų ir palaiko jų taikymą:

10.1.1 P01 – Informacijos saugumo politika: nustato saugumo informuotumą kaip bazinę kontrolės priemonę organizacijos ISVS.

10.1.2 P03 – Priimtino naudojimo politika: reikalauja naudotojo patvirtinimo mokymų metu ir aiškiai apibrėžia atsakomybes, susijusias su kasdieniu technologijų naudojimu.

10.1.3 P07 – Įdarbinimo ir darbo santykių nutraukimo politika: užtikrina, kad mokymai būtų integruoti darbo pradžioje ir stebimi viso darbo laikotarpiu.

10.1.4 P06 – Rizikos valdymo politika: susieja į žmogų orientuotus mokymus su grėsmių modeliavimu ir liekamosios rizikos mažinimo strategijomis.

10.1.5 P33 – Audito ir atitikties stebėsenos politika: patvirtina, kad informuotumo kontrolės priemonės auditų metu yra veikiančios, išmatuojamos ir veiksmingos.

10.2 Kartu šios politikos sudaro išsamią elgsenos kontrolės sistemą, integruojančią informuotumą, atskaitomybę ir organizacinės kultūros stiprinimą.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 7.3 skyrius – Informuotumas: reikalauja, kad organizacijos užtikrintų, jog darbuotojai žinotų informacijos saugumo politikas ir savo atsakomybes. Ši politika šį reikalavimą įgyvendina per struktūrizuotą įdarbinimą, periodinius mokymus ir išmatuojamą dalyvavimą kampanijose.

11.1.2 A priedo kontrolė 6.3 – Informacijos saugumo supratimas, švietimas ir mokymai: visiškai įgyvendinama per pradinius, vaidmenimis grindžiamus ir tęstinius mokymų programos elementus, pritaikytus naudotojų rizikos profiliams.

11.2 ISO/IEC 27002:2022 – Kontrolė 6

11.2.1 Palaiko pagal pareigas tinkamų informuotumo mokymų kūrimą ir teikimą, akcentuojant saugaus elgesio stiprinimą ir periodinius atnaujinimus pagal grėsmių žvalgybą ir audito grįžtamąjį ryšį.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1–AT-5 (informuotumo ir mokymų šeima): ši politika atitinka AT-1 (politika ir procedūros), AT-2 (informuotumo mokymai), AT-3 (vaidmenimis grindžiami mokymai), AT-4 (saugumo mokymų įrašai) ir AT-5 (ryšys su saugumo grupėmis).

11.3.2 IA-5, AC-2: stiprina naudotojų atsakomybę už saugų autentifikavimą ir priimtino naudojimo principų laikymąsi – tai pagrindiniai informuotumo programų elgsenos rezultatai.

11.3.3 IR-1–IR-8: pasirengimas reaguoti į incidentus stiprinamas per tikslines informuotumo kampanijas ir simuliacijas.

11.4 ES BDAR (2016/679)

11.4.1 32 straipsnis – Tvarkymo saugumas: nustato, kad darbuotojai, tvarkantys asmens duomenis, turi būti apmokyti atpažinti, užkirsti kelią ir pranešti apie rizikas asmens duomenims. Ši politika užtikrina, kad duomenų tvarkytojai ir visi susiję vaidmenys būtų atitinkamai apmokyti.

11.4.2 39 straipsnis – Duomenų apsaugos pareigūno užduotys: apima informuotumo didinimą ir darbuotojų, dalyvaujančių tvarkymo operacijose, mokymą.

11.4.3 78 konstatuojamoji dalis: skatina taikyti tinkamas informuotumo priemones, siekiant užtikrinti patikimas saugumo praktikas ir politikos laikymąsi.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21(2)(a, b) straipsnis: reikalauja, kad subjektai patvirtintų rizikos analizės ir saugumo mokymų politikas visam susijusiam personalui. Ši politika šį reikalavimą įgyvendina nustatydama nuolatinius, vaidmenų jautrumą rizikai atitinkančius mokymų procesus.

11.5.2 21(3) straipsnis: skatina didinti kibernetinio saugumo rizikos informuotumą tarp vadovybės ir darbuotojų per informuotumo iniciatyvas ir simuliacijas.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 13 straipsnis – Skaitmeninio operacinio atsparumo strategija: nustato, kad IRT rizikos informuotumas ir mokymai turi būti valdysenos modelio dalis. Ši politika užtikrina, kad su žmonėmis susijusi rizika būtų valdoma nuolatiniu švietimu ir grėsmių simuliacijomis.

11.6.2 5 ir 8 straipsniai: pabrėžia vidaus kontrolės sistemų svarbą, kurių pamatiniai komponentai IRT atsparumui ir kibernetinei higienai yra informuotumas ir mokymai.

11.7 COBIT 2019

11.7.1 APO07 – Valdomi žmogiškieji ištekliai: stiprina poreikį ugdyti informuotumą apie saugumo atsakomybes ir integruoti tai į darbuotojų valdymą.

11.7.2 DSS05 – Valdomos saugumo paslaugos: nustato naudotojų švietimo ir incidentų pranešimo kontrolės priemones, kurios yra neatsiejama šios politikos dalis.

11.7.3 MEA03 – Stebėti, vertinti ir įvertinti atitiktį: reikalauja peržiūrėti naudotojų elgsenos ir politikos laikymosi veiksmingumą – šioje politikoje tai įgyvendinama per fišingo testus, testus ir informuotumo kampanijų rodiklius.