DARBO SU AB „LIETUVOS DRAUDIMAS“ INFORMACINĖMIS SISTEMOMIS TAISYKLĖS (išrašas iš Politikos)

Terminai ir apibrėžimai

Sąvoka, trumpinys	Apibrėžimas
ICSP	Informacijos ir kibernetinio saugumo politika.
Bendrovė	AB „Lietuvos draudimas“ (įskaitant Estijos filialą).
LD	AB „Lietuvos draudimas“ (neįskaitant Estijos filialo).
Grupė	„PZU“ grupė.
Partneris	Fizinis ar Juridinis asmuo, siejamas su LD sutartiniais santykiais ir besinaudojantis LD informacinėmis sistemomis
ICT	Informacinių ir ryšio technologijų turtas (programinė arba techninė įranga, naudojama Partnerio veikloje).
I/D	Informacijos ir duomenų turtas (saugotini materialieji arba nematerialieji informaciniai ar duomenų rinkiniai).
Konfidencialumas	Savybė, užtikrinanti, kad nei I/D, nei ICT nėra prieinamas ar atskleistas neįgaliotiems asmenims, subjektams, procesams ar sistemoms.
Vientisumas	Tikslumo ir išsamumo savybė.
Prieinamumas	Savybė, užtikrinanti prieinamumą įgaliotam subjektui ir galimybę naudotis pagal poreikį I/D, ICT (savalaikiškumas).
	.
	.
CSM	Kibernetinio saugumo vadovas Baltijos šalims.
Kibernetinė ataka	Bet kokio tipo įsilaužimas į ICT atliekant kenksmingus / kenkėjiškus bandymus sunaikinti, atskleisti, pakeisti, deaktyvinti, pavogti informacinį turtą ar gauti prie jo neautorizuotą prieigą ar neautorizuotai juo pasinaudoti.
ICS	Informacijos ir kibernetinis saugumas.
Kibernetinis saugumas	I/D, ICT konfidencialumo, vientisumo ir prieinamumo užtikrinimas kibernetinėje erdvėje.
Informacijos saugumas	I/D konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Be to, turėtų būti atsižvelgta ir kitas savybes, pavyzdžiui, autentiškumą, atskaitomybę, neatsisakymą ir patikimumą.
Projektas	Bet koks projektas ar jo dalis, kurį įgyvendinant keičiamas, pakeičiamas ar įdiegiamas ICT.
ICT paslaugos	Vienam ar keliems vidaus arba išorės ICT sistemų vartotojams teikiamos paslaugos.
ICT sistemos	I/D, ICT, paslaugų ar kitų informacijos tvarkymo komponentų rinkinys, įskaitant veiklos aplinką, padedančią verslui pasiekti konkrečius verslo tikslus.
Pažeidžiamumas	I/D, ICT ar jų valdymo silpnoji vieta, neatsparumas ar trūkumas, kuriais gali būti pasinaudota susidūrus su viena ar daugiau grėsmių.
AUP	Priimtino naudojimo politika.
Loginis	Loginis sluoksnis apima logines ICT savybes. Jį sudaro vieną su kitu ICT siejantys loginiai ryšiai.
Fizinis	Fizinis sluoksnis apima geografines/aplinkos ir fizines ICT savybes . Geografinės/aplinkos savybės visada nurodo fizinę ICT buvimo vietą ir su ja susijusią aplinką (klimatas ir pan.), o fizinės ICT savybės nurodo fizinius (materialius) ICT veiksnius.
Užsakovas	Bendrovės klientas.
Prieiga	Suteikta teisė naudotis I/D ar ICT loginiu / tinklo būdu.
Vartotojas	Partneris, besinaudojantis kitu ICT verslo / darbo pareigoms vykdyti.
Vartotojo ID	Loginės Vartotojo tapatybės nustatymo priemonės (pvz. Vartotojo paskyra įmonės ICT sistemoje).
	.

Saugomas I/D	I/D priklausantis Konfidencialių, Jautrių ar Asmens (BDAR) I/D tipui.
EBA	EBA/GL/2019/04 gairės.
2FA	Antras autentiškumo patvirtinimo veiksnys.

Politika

Tikslas

Užtikrinti priimtiną Informacijos ir duomenų (I/D) bei Informacinių ir ryšių technologijų (ICT) naudojimą.

1. Įvadas

1.1. Šioje Politikoje nustatyti būtiniausieji reikalavimai dėl priimtino (tinkamo) I/D ir ICT naudojimo. Šios Politikos nuostatos parengtos laikantis ICSP nustatytų reikalavimų.

2. Apibrėžtis ir taikymo sritis

1.2. Apibrėžtis

1.2.1. Šioje Politikoje nustatyti būtiniausieji reikalavimai dėl priimtino Bendrovės I\D ir ICT naudojimo. Šios Politikos nuostatos apibrėžtos pagal ICSP nustatytus reikalavimus.

1.3. Taikymo sritis

1.3.1.1. Politika tiesiogiai taikoma Partneriams.
kurie gali prieiti arba naudotis Bendrovės I/D, ICT ir kelti riziką Bendrovės I/D, ICT konfidencialumui, vientisumui ir prieinamumui (loginiai ir fiziniai lygmenys) – jei jie yra įpareigoti laikytis šios Politikos reikalavimų raštu.

1.3.1.2. visiems Bendrovės loginiams ir fiziniams I/D, ICT, nesvarbu, ar jie būtų saugomi, perduodami ar naudojami.

3. Politikos reikalavimai

3.1. Bendrojo I/D, ICT naudojimo politika

3.1.1. Bendrasis principas – Bendrovės / Grupės saugomi I/D, ICT turi būti naudojami laikantis šios Politikos ir atitinkamų teisės aktų reikalavimų. Partneriai yra atsakingi užtikrinti I/D ir ICT Fizinį ir Loginį saugumą, Konfidencialumą, Vientisumą ir Prieinamumą (ICS).

3.1.2. Bendrasis principas – Bendrovės / Grupės I/D turi būti naudojami tik su bendradarbiavimu su bendrove susijusioms užduotims vykdyti; Draudžiama jais naudotis asmeninėms reikmėms.

3.1.3. Bendrasis principas – būtina imtis visų reikalingų priemonių, siekiant apsaugoti Bendrovės / Grupės klientus nuo Saugomų I/D nutekėjimo, tapatybės vagystės ir finansinių nuostolių.

3.1.4. Bendrasis principas – draudžiama daryti Saugomų I/D kopijas, nuotraukas, vaizdo ar garso įrašus. Tai leidžiama tuo atveju, jei tai yra tiesiogiai susiję su bendradarbiavimu su Bendrove arba Bendrovės / Grupės interesais.

3.1.5. Bendrasis principas – siekdama vykdyti (atitikti) Grupės, Bendrovės ar Lietuvos Respublikos teisės aktus, pagal kuriuos reikalaujama apsaugoti I/D, ICT, Bendrovė gali pasinaudoti savo teise tikrinti su Bendrovės I/D ICT susijusius žurnalų įrašus.

3.1.6. Bendrasis principas – su jumis telefonu ar el. paštu susisiekus IT pagalbos tarnybos atstovui, įsitikinkite, kad asmuo skambina iš telefono numerio +370 5 2742030 arba rašo iš el. pašto adreso pagalba@ld.lt. Priešingu atveju užsirašykite telefono numerį ar el. pašto adresą ir nedelsdami nutraukite tokį kontaktą. Apie tokį įvykį informuokite kaip apie saugumo incidentą.

3.1.8. Bendrasis principas – esant abejonių dėl leistino I/D, ICT naudojimo Partneris turi kreiptis į pagalba@ld.lt.

3.1.9. Bendrasis principas – nesilaikant šios Politikos bus taikomos sankcijos, priklausančios nuo Patnerio padarytos žalos.

3.2. I/D naudojimo, perdavimo ir tvarkymo politika

3.2.1.	Saugomi I/D turi būti naudojami laikantis Konfidencialios informacijos saugojimo ir supažindinimo su ja tvarkos
3.2.2.	Asmens (Saugomi) I/D turi būti naudojami pagal Asmens duomenų teisinės apsaugos tvarką
3.2.3.	Bet koks keitimasis I/D (įskaitant per socialinius tinklus) turi atitikti Reputacijos ir išorės komunikacijos politiką.
3.2.4.	Be Savininko leidimo draudžiama atskleisti Bendrovės / Grupės I/D Trečiosioms šalims.
3.2.5.	Dirbdamas su apsaugotais I/D kompiuteryje (įskaitant išmaniuosius telefonus, planšetinius kompiuterius ir kitus ICT) ar perduodamas tokius I/D telefonu, Partneris privalo imtis priemonių, kad ICT ekrane rodomų I/D negalėtų matyti ar girdėti neįgaliotas asmuo.

3.2.8.	Draudžiama saugoti ar tvarkyti Bendrovės / Grupės I/D ilgiau, nei tai yra būtina.
3.2.9.	Asmeninės / viešosios internetinės failų saugyklos neturi būti naudojamos Bendrovės / Grupės I/D saugoti ar persiųsti, taip pat Bendrovės / Grupės verslo reikalais.
3.2.10.	Draudžiama palikti balso pranešimus, kuriuose minimi apsaugoti I/D, telefono atsakikliuose. Draudžiama siųsti teksto pranešimus, kuriuose minimi apsaugoti I/D tam autorizacijos neturinčioms šalims.
3.2.11.	I/D gali būti perduodami įvairiais ICT, įskaitant el. paštu, balso paštu, faksu, vaizdo priemonėmis ir pan. Partneris turi užtikrinti, kad perduodant I/D būtų laikomasi šios Politikos.
3.2.12.	Draudžiama be viešųjų ryšių padalinio atstovo leidimo skelbti komentarus apie Bendrovės / Grupės verslą bet kokiose interneto svetainėse ar tarnybose.
3.2.13.	Draudžiama komentuoti bet kokį subjektą, asmenį, gaminį ar paslaugą netiksliu, nepagrįstu, netinkamu, neteisingu ar diskredituojančiu būdu tiek Bendrovėje (Grupėje), tiek už jos ribų.
3.2.14.	Draudžiama piktnaudžiauti autorių teisių saugomais I/D ar kitais autoriniais darbais.
3.2.15.	Draudžiama naudojantis Bendrovės / Grupės ICT perduoti, saugoti, kurti, valdyti ar kopijuoti toliau pateiktų kategorijų I/D:
3.2.15.1.	užgaulaus, šmeižikiško, bauginančio, žeminančio, trikdančio, gąsdinančio ar neteisėto pobūdžio;
3.2.15.2.	diskriminuojančio rasės, lyties, amžiaus ir kt. pagrindu pobūdžio;
3.2.15.3.	pornografinio ar nepadoraus pobūdžio;
3.2.15.4.	apsaugoti autorių teisių (darbai, kuriems nesuteiktas autoriaus leidimas, ar darbai, kuriais pažeidžiamos autorių ir intelektinės nuosavybės teisės);
3.2.15.5.	įžeidžiančio, ypač Bendrovės / Grupės logotipo ar pavadinimo atžvilgiu, pobūdžio.

3.7. Nuotolinio darbo politika

3.7.1.	Nuotolinis darbas reiškia visas darbo ne biure formas, įskaitant netradicines darbo aplinkas, pavyzdžiui, vadinamą darbu naudojantis nuotolinėmis telekomunikacijos priemonėmis, „lanksčia darbo vieta“, nuotolinio ar virtualaus darbo aplinkomis. Dirbdamas nuotoliniu būdu Partneris yra visiškai atsakingas už šioje Politikoje nustatytų reikalavimų laikymąsi. Jei dirba nuotoliniu būdu, Partneris privalo užtikrinti nuotolinio darbo atitiktį Fizinio saugumo politikos reikalavimams.
3.7.3.	Dirbdamas nuotoliniu būdu Partneris privalo vykdyti šioje Politikoje ir, jei taikytina, ICSP nustatytus reikalavimus.
3.7.4.	Partneris privalo laikytis reikalavimo, kad šeimos nariai ar draugai yra laikomi neautorizuotais subjektais ir neturi teisės naudoti, žinoti ar gauti prieigą prie Bendrovės / Grupės I/D, ICT.s
3.7.5.	Partneriui draudžiama bandyti iššifruoti Bendrovės virtualiojo privataus tinklo (VPN) srautą ar prijungti neautorizuotus ICT prie Bendrovės / Grupės ICT
3.7.6.	Bendrovė draudžia dirbti nuotoliniu būdu naudojantis nesaugiais privačiais ir viešaisiais tinklais Jungdamasis prie Bendrovės tinklų vartotojas privalo visada naudotis VPN ryšiu. PASTABA: Kai kuriose mobiliuosiuose ICT, pavyzdžiui, išmaniuosiuose telefonuose, minėtas VPN ryšys šiuo metu nėra palaikomas, todėl ICT (taikomosios programėlės, įdiegtos išmaniajame telefone), turintys prieigą prie Bendrovės ICT, privalo užtikrinti būtiną perduotų ir gautų I/D apsaugos lygį

3.8. Prieigos prie I/D, ICT suteikimo politika

3.8.1. Jei Partneris pageidauja naudoti Bendrovės / Grupės I/D, ICT (sistemas, kompiuterius, paslaugas ir pan.), jiems turi būti suteikta prieiga (autorizacija prieiti) prie I/D, ICT, bei patvirtinti prieigos atributai ir teisės. Prieigos atributai yra Vartotojo ID, slaptažodis, tam tikrais atvejais – antras autentiškumo patvirtinimo veiksnys (2FA), pvz., PIN kodas. Prieigos teisės apima leidimą pasinaudoti įvairiais I/D ir ICT.

3.8.2. Norėdami gauti prieigos atributus / teises, susisiekite su savo tiesioginiu vadovu / sutarties savininku. PASTABA: Prieiga prie Bendrovės ICT suteikiama pagal IS naudotojų teisių valdymo procedūrą ir laikantis ICSP nustatytų reikalavimų. Suteikiant minėtoje procedūroje nenumatytas prieigos teises turi būti laikomasi savininkų nustatytų taisyklių, neprieštaraujančių ICSP. Prieiga suteikiama tik laikantis „Reikia žinoti“ principo. Partneriui turi būti pasiekiama tik tiek I/D, kiek būtina.

3.8.3. Norėdamas prisijungti prie ICT, Partneris turi atlikti prisijungimo procedūrą. Prisijungimo metu būtina įvesti unikalų Vartotojo ID (identifikacija), įsimintą slaptažodį (autentiškumo patvirtinimas) ir jei reikia – 2FA. PASTABA: Draudžiami bet kokie neautorizuoti bandymai prisijungti prie Bendrovės / Grupės ICT ar jais pasinaudoti.

3.8.5. Draudžiama atskleisti Vartotojo ID ir (arba) slaptažodį / 2FA kitam asmeniui / šaliai ar naudoti kito subjekto Vartotojo ID ir slaptažodį / 2FA.

3.8.6. Slaptažodžių (įskaitant PIN kodus) saugumas:

3.8.6.1. Draudžiama naudoti tuos pačius ar vienodus slaptažodžius / 2FA / PIN kodus išoriniuose ICT (nepriklausančiuose Bendrovei / Grupei);

3.8.6.2. Draudžiama atskleisti slaptažodžius / 2FA / PIN kodus kitiems subjektams.

3.8.6.3. Slaptažodžius / 2FA / PIN kodus būtina įsiminti. Draudžiama juos laikyti užrašytus (elektroninėje ar popierinėje laikmenoje);

3.8.6.4. Laikinuosius slaptažodžius / 2FA / PIN kodus privaloma pakeisti po pirmojo prisijungimo;

3.8.6.5. Mažiausias privalomas slaptažodžių sudėtingumas:
Vartotojo slaptažodžius turi sudaryti bent 14 simbolių.
Slaptažodžius turi sudaryti didžioji ir mažoji raidės, skaičiai ir specialieji simboliai. Slaptažodžių negali sudaryti lietuviško, estiško, rusiško, lenkiško, latviško, lotyniško ar angliško žodyno žodžiai (pvz., P@ssword1, V!lnius2018 ir t. t.) bei lengvai nuspėjamos sekos (pvz., qwerty, ABC123!@# ir pan.);

3.8.6.6. Mažiausias 2FA sudėtingumas yra keturi nepasikartojantys simboliai;

3.8.6.7. Mažiausias PIN kodų sudėtingumas yra keturi nepasikartojantys simboliai;

3.8.6.8. Slaptažodžius / PIN kodus reikia keisti kas 6 mėnesius (kur yra techninės galimybės, ICT Vartotojas bus paragintas tai atlikti arba Vartotojas turi pats prisiminti, kad būtina pakeisti slaptažodį / PIN kodą rankiniu būdu);

3.8.6.9. Įvedami slaptažodžiai / PIN kodai neturi būti matomi kitiems asmenims.

3.9. Švaraus stalo ir švaraus ekrano politika

3.9.1. Švaraus stalo / švaraus ekrano politika skirta sumažinti riziką, keliamą neteisėtos prieigos prie I/D, ICT, jų praradimo ir sugadinimo. Partneris privalo užtikrinti, kad Saugomi I/D niekada nebūtų paliekami neapsaugoti (nesaugūs), pavyzdžiui, kad neįgalioti subjektai negalėtų perskaityti (ar pasinaudoti) I/D iš ekranų ar popierine forma, taip pat kad jų nebūtų galima pavogti tuo metu, kai jie yra saugomi nešiojamuosiuose ICT ir pan.
PASTABA: Fiziniai švaraus stalo ir švaraus ekrano politikos reikalavimai išsamiai aprašyti Fizinio saugumo politikoje, o ICS reikalavimai yra išvardyti toliau.

3.9.2. Saugomus I/D reikia visada tvarkyti laikantis I/D klasifikacijos, teisinių / sutartinių reikalavimų, taip pat šios Politikos reikalavimų, įskaitant I/D Savininkų nustatytus reikalavimus. Reikėtų atsižvelgti į šias rekomendacijas:

3.9.2.1. Be priežiūros palikti kompiuteriai ir nešiojamieji ICT privalo būti išjungti arba paliekami nuo jų atsijungus ar užrakinus ekrano ir klaviatūros rakinimo mechanizmu, valdomu slaptažodžiu / PIN kodu ar biometrine žyma;

3.9.2.2. Jei kompiuteriais ir nešiojamaisiais ICT nesinaudojama ilgiau nei 1 val., juos privalu išjungti.

3.10. Vartotojų veiklos stebėsenos politika

3.10.1.	Siekdama vykdyti ICSP, Bendrovės / Grupės ar Lietuvos Respublikos teisinius reikalavimus, Bendrovė stebi Partnerių veiklą, susijusią su Bendrovės ICT.
3.11.	**Incidentų valdymo ir informavimo apie juos politika**
3.11.1.	Partneriai, pastebėję ar įtarę ICS incidentą, privalo nedelsiant apie tai informuoti IT pagalbos tarnybą pagalba@ld.lt, tel. +370 5 2742030.
3.11.2.	Partneriai, sužinoję apie galimą ICS pažeidžiamumą, privalo nedelsiant apie tai informuoti IT pagalbos tarnybą pagalba@ld.lt, tel. +370 5 2742030.
3.12.	**Informuotumo didinimo ir mokymo ICS klausimais politika**
3.12.1.	Partneriai privalo edukuotis ir kelti kvalifikaciją ICS klausimais veikloje, kad užtikrintų reikiamą įgūdžių ir žinių ICS srityje lygį.
3.13.	**I/D atsarginio kopijavimo politika**
3.13.1.	ID, esančių Personalo / Partnerių ICT (kompiuteriai ir išmanieji telefonai), atsarginės kopijos nėra daromos, todėl nelaimingo atsitikimo atveju jie gali būti prarasti. Visi svarbūs I/D turi būti saugomi saugiuose ICT (Bendrovės tarnybinėse stotyse ar sistemose).
4.	**Pareigos ir atsakomybė**
4.9.	Politikos Savininkas (CSM) yra atsakingas įgyvendinti Politiką pagal galiojančius teisinius reikalavimus;
4.10.	Rizikos valdymo funkcija yra atsakinga vykdyti Politikos rengimo ir įgyvendinimo priežiūrą.
4.11.	Personalas / Partneriai privalo informuoti apie bet kokią keliamą riziką ir Politikos pažeidimus IT pagalbos tarnybą pagalba@ld.lt, tel. +370 5 2742030.

DARBO SU AB „LIETUVOS DRAUDIMAS“ goLD INFORMACINE SISTEMA ATMINTINĖ

VERSIJA 0.2

Prie goLD sistemos jungiamasi adresu https://go.ld.lt/ Prisijungimui naudojant naujausią interneto naršyklės versiją (pvz., Mozilla Firefox, Google Chrome, Microsoft Edge).

Prisijungti prie goLD sistemos galima dviem būdais:

1. Naudojant Prisijungimo vardą ir SMS/EMAIL kodą.

Įvedami šie duomenys:

a. Prisijungimo vardas – nekintamas ženklų rinkinys, skirtas identifikuoti Jus sistemoje, suteikiamas „Lietuvos draudimo“.

b. Slaptažodis – Jūsų susikurtas, saugumo taisykles atitinkantis slaptažodis.

Įvedus šiuos duomenis, galite pasirinkti gauti patvirtinimo kodą SMS žinute arba el. paštu. Pasirinkus vieną iš variantų, gausite patvirtinimo kodą į Jūsų vartotojo kortelėje “Lietuvos draudimo” duomenų bazėje nurodytą mobilųjį telefoną arba el. paštą (atitinkamai pagal pasirinkimą).

Įvedus gautą patvirtinimo kodą būsite prijungti prie sistemos.

2. Naudojant Prisijungimo vardą ir mobilųjį parašą.

Įvedami šie duomenys:

a. Prisijungimo vardas – nekintamas ženklų rinkinys, skirtas identifikuoti Jus sistemoje, suteikiamas „Lietuvos draudimo.

b. Mobiliojo telefono numeris – įvedamas telefono numeris turi sutapti su numeriu, įrašytu Jūsų vartotojo kortelėje “Lietuvos draudimo” duomenų bazėje.

Įvedus šiuos duomenis, į savo mobilųjį telefoną gausite kodą, kuris turi sutapti su goLD prisijungimo lange matomu kodu. Patvirtinus šį kodą m. parašu būsite prijungti prie sistemos.

Slaptažodžio keitimo, priminimo funcionalumai veikia goLD sistemoje.