DARBO SU AB „LIETUVOS DRAUDIMAS“ INFORMACINĖMIS SISTEMOMIS TAISYKLĖS (išrašas iš Priimtino naudojimo politikos)

Terminai ir apibrėžimai

Sąvoka, trumpinys	Apibrėžimas
Bendrovė	AB „Lietuvos draudimas“ (įskaitant Estijos filialą).
LD	AB „Lietuvos draudimas“ (neįskaitant Estijos filialo).
Estijos filialas (EE)	AB „Lietuvos draudimas“ Estijos filialas.
Grupė	„PZU“ grupė.
IRT turtas	Programinė arba aparatinė įranga, Bendrovės naudojama tinklų ir informacinėse Sistemose.
Informacinis turtas	Materialios arba nematerialios informacijos, kurią verta apsaugoti, rinkinys.
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).
Autentiškumas	Teisingumas, tikrumas.
BDAR	Bendrasis duomenų apsaugos reglamentas
Rizikos funkcija / rizikos valdymo funkcija	Suprantama taip, kaip nustatyta Rizikos valdymo strategijoje.
Atitikties funkcija	Suprantama taip, kaip nustatyta Atitikties politikoje.
Administratoriaus paskyra	Vardinė paskyra sukurta konkrečiam vartotojui, skirtinga negu aktyvios direktorijos paskyra (AD) skirta atlikti specifinėms administravimo funkcijoms (pvz., Oracle duomenų bazių administratorius)
Techninė paskyra	Nevardinė paskyra naudojama verslo sistemose, monitoringo sistemose automatiniams procesams vykdyti, pvz., duomenų apsikeitimas, skaitymas
Sisteminė paskyra	Nevardinė paskyra sukuriama automatiškai sistemos instaliavimo/ konfigūravimo metu, pvz., root paskyra linux sistemoje
Techninis administratorius	IT administratorius kuris konkrečiai suveda vartotoją ir slaptažodį į veiklos sistemos techninės paskyros rekvizitus
Verslo administratorius	Veiklos funkcijų administratorius, kuriam būtina techninė paskyra konkrečios veiklos sistemos ar paslaugos tinkamam funkcionavimui
SLA	Susitarimas dėl paslaugos (kokybės) lygmens.
Savininkas	Asmuo ar subjektas, kuriam patikėta atsakomybė už I/D, ICT ir atitinkami įgaliojimai. Patikslinimas: LD ar EE departamento direktorius ar padalinio vadovas, kurio atsakomybės srityje dažniausiai naudojamas I/D ir ICT.
Bendrovės vadovybė	LD departamentų direktoriai, EE padalinio direktorius ir departamentų vadovai.
ITDEP	LD Operacijų ir IT departamentas ir EE IT ir pokyčių departamentas.
CSM	Kibernetinio saugumo vadovas Baltijos šalims.
ITD	LD Operacijų ir IT departamento direktorius ir (arba) EE padalinio IT ir pokyčių departamento vadovas.
Kibernetinis incidentas / išpuolis	Su IRT susijęs piktavališkas incidentas, kuris yra sukeliamas, kai priešiškas subjektas atlieka veiksmus siekiant sunaikinti, atskleisti, pakeisti, išjungti, pavogti ar įgyti neteisėtą prieigą prie bet kokio turto arba neteisėtai juo naudotis.
ICS	Informacijos ir kibernetinis saugumas

Kibernetinis saugumas	Visa veikla, būtina tinklams ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių.
Informacijos saugumas	informacinio turto konfidencialumo, vientisumo, autentiškumo ir prieinamumo užtikrinimas.
Kibernetinė grėsmė	Galima aplinkybė, įvykis arba veiksmas, kuris galėtų pažeisti, sutrikdyti arba kitaip neigiamai paveikti tinklų ir informacines sistemas, tokių sistemų naudotojus ir kitus asmenis.
IRT paslaugos	Skaitmeninės ir duomenų paslaugos, nuolat teikiamos naudojantis IRT sistemomis vienam ar keliems vidaus ar išorės naudotojams, įskaitant aparatinę įrangą kaip paslaugą ir aparatinės įrangos paslaugas, kurios apima techninės paramos teikimą, aparatinės įrangos teikėjui atliekant programinės įrangos arba programinės aparatinės įrangos atnaujinimus, išskyrus tradicines analoginio telefono ryšio paslaugas.
Tinklų ir informacinė sistema	a) Elektroninių ryšių tinklas - – perdavimo sistemos, tiek grindžiamos, tiek negrindžiamos nuolatine infrastruktūra arba centralizuoto valdymo pajėgumais, ir atitinkamais atvejais komutavimo ar maršruto parinkimo įranga bei kiti ištekliai, įskaitant neaktyvius tinklo elementus, kurie leidžia perduoti signalus laidais, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuoto (linijų ir paketų komutavimo, įskaitant internetą) ir judriojo ryšio tinklus, elektros perdavimo kabelines sistemas, tokiu mastu, kokiu jos yra naudojamos signalams perduoti, radijo ir televizijos programų transliavimui naudojami tinklai ir kabelinės televizijos tinklai, neatsižvelgiant į perduodamos informacijos pobūdį b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.
Įsilaužimo (įsiskverbimo) į informacinę ir ryšių įrangą testavimas (angl. Pen-test)	Kontroliuojamas bandymas pažeisti objekto kibernetinį atsparumą simuliuojant tikrų nusikaltėlių taktiką, metodus ir procedūras. Jis grindžiamas tikslinėmis žiniomis apie galimas grėsmes ir yra nukreiptas į subjekto žmones, procesus ir technologiją, su minimaliu prognozavimu ir poveikiu veiklai.
Pažeidžiamumas	Turto, sistemos, proceso ar kontrolės priemonės silpnoji vieta, jautrumas ar trūkumas, kuriais gali būti pasinaudota.
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.
Personalas	Bendrovės darbuotojai ar pagal sutartis samdomi asmenys, veikiantys kaip darbuotojai.
NDA	Konfidencialumo susitarimas.
Prieiga	Suteikta teisė naudotis informaciniu ar IRT turtu loginiu / tinklo būdu
Tinklas	Duomenų perdavimo tinklas (loginis ir fizinis).
Vartotojas	Personalo narys ar IRT, besinaudojantis kitu IRT verslo / darbo pareigoms vykdyti.
Vartotojo ID	Loginės Vartotojo tapatybės nustatymo priemonės (pvz. Vartotojo paskyra įmonės ICT sistemoje).
Kenkėjiškas programinis kodas	Programinė įranga, specialiai sukurta sutrikdyti ICT veikimą, taip pat sugadinti ar gauti neautorizuotą prieigą prie ICT.
Trečioji šalis	Pagal sutartį pasamdyta ar kitaip Bendrovės verslo veikloje dalyvaujanti šalis.
OWASP	Atvirųjų interneto taikomųjų programų saugumo užtikrinimo projektas yra pelno nesiekiantis fondas, siekiantis pagerinti programinės įrangos saugumą. Vykdantis bendruomenių inicijuojamus atvirojo kodo programinės įrangos projektus, visame pasaulyje turintis šimtus vietos padalinių, buriantis dešimtis tūkstančių narių ir rengiantis edukacines ir mokomąsias konferencijas OWASP fondas aprūpina kūrėjus ir technologijų specialistus ištekliais, būtinais žiniatinkliui apsaugoti.
VPN	Virtualus privatusis tinklas.

Saugomas informacinis turtas	Informacinis turtas priklausantis Konfidencialių, Jautrių ar Asmens duomenų (BDAR) informacinio turto tipui.
EBA	EBA/GL/2019/04 gairės.
2FA	Antras autentiškumo patvirtinimo veiksnys.

Politika

Tikslas

Užtikrinti priimtiną Informacijos ir duomenų bei Informacinių ir ryšių technologijų naudojimą.

1. Įvadas

1.1. Šioje Politikoje nustatyti būtiniausieji reikalavimai dėl priimtino (tinkamo) Informacijos ir IRT turto naudojimo. Šios Politikos nuostatos parengtos laikantis ICSP nustatytų reikalavimų.

2. Apibrėžtis ir taikymo sritis

2.1 Apibrėžtis

2.1.1 Šioje Politikoje nustatyti būtiniausieji reikalavimai dėl priimtino Bendrovės Informacinio/IRT turto naudojimo. Šios Politikos nuostatos apibrėžtos pagal ICSP nustatytus reikalavimus.

2.2 Taikymo sritis

2.2.1 Politika tiesiogiai taikoma:

2.2.1.1 Visiems Bendrovės darbuotojams, Stebėtojų tarybos nariams ir Valdybos nariams, draudimo tarpininkams (draudimo brokeriams ir draudimo agentams), Grupės darbuotojams, dirbantiems Bendrovėje (toliau šioje Politikoje visi kartu ir kiekvienas atskirai vadinami „Darbuotojais“ ar „Personalu“); Politikos priedas taikomas tik Bendrovės Estijos filialui.

2.2.1.2 Trečiosioms šalims (paslaugų teikėjams, partneriams ir visiems kitiems subjektams), kurios gali naudotis Bendrovės Informaciniu ir IRT turtu ir kelti riziką Bendrovės Informacinio ir IRT turto konfidencialumui, vientisumu, autentiškumuii ir prieinamumui (loginiai ir fiziniai lygmenys) – jei jos yra įpareigotos laikytis šios Politikos reikalavimų raštu (toliau šioje Politikoje visi kartu ir kiekvienas atskirai vadinami „Trečiosiomis šalimis“).

2.2.2 Visam Bendrovės Informaciniam ir IRT turtui, nesvarbu, ar jis būtų saugomas, perduodamas ar naudojamas

3. Politikos reikalavimai

3.1. Bendrojo informacinio/IRT turto naudojimas

3.1.1. Bendrasis principas – Bendrovės / Grupės saugomas Informacinis/IRT turtas turi būti naudojamas laikantis šios Politikos ir atitinkamų teisės aktų reikalavimų. Darbuotojai ir Trečiosios šalys yra atsakingi užtikrinti Informacinio/IRT turto fizinį ir loginį saugumą, konfidencialumą, vientisumą, autentiškumą ir prieinamumą.

3.1.2. Bendrasis principas – Bendrovės / Grupės informacinis/IRT turtas turi būti naudojami tik su darbu susijusioms užduotims vykdyti; draudžiama jais naudotis asmeninėms reikmėms.

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

3.1.4. Bendrasis principas – draudžiama Bendrovės / Grupės patalpose daryti saugomo informacinio turto kopijas, nuotraukas, vaizdo ar garso įrašus. Tai leidžiama tuo atveju, jei tai yra tiesiogiai susiję su darbo pareigomis arba Bendrovės / Grupės interesais.

3.1.5. Bendrasis principas – siekdama vykdyti (atitikti) Grupės, Bendrovės ar Lietuvos Respublikos (EE padalinyje – Estijos Respublikos) teisės aktus, pagal kuriuos reikalaujama apsaugoti Informacinį/IRT turtą, Bendrovė, esant pagrįstų įtarimų, kad darbuotojas nesilaiko teisės aktų ar Bendrovės tvarkų reikalavimų, gali pasinaudoti savo teise tikrinti telefono skambučių ar kitus registracijos žurnalus ar informacinį/IRT turtą, kuris buvo priskirtos Personalui ar Trečiajai šaliai.

3.1.6. Bendrasis principas – jei su Darbuotoju telefonu ar el. paštu susisiekus IT pagalbos tarnybos atstovui, kyla įtarimų dėl bendravimo autentiškumo, pokalbį reikia nutraukti ir perskambinti bendruoju IT pagalbos telefonu ar persiusti žinutę jei kontaktuojama el. paštu . Jokie prašymai atskleisti prisijungimo rekvizitus, slaptažodžius, PIN kodus, ar kitą informaciją naudojama darbuotojo identifikavimui ar prisijungimui negalimi.

	Skambučio atveju, kilus įtarimams privaloma užsirašyti telefono numerį ir nedelsdami nutraukti tokį pokalbį. Apie įvykį reikia informuoti kaip apie saugumo incidentą. Tik IT pagalbos tarnybai leidžiama konfigūruoti / taisyti Personalui priskirtus IRT.
3.1.7.	Bendrasis principas – draudžiama su darbu susijusiais, konfidencialiais reikalais kalbėtis viešosiose vietose, atviro tipo biuruose ir neapsaugotose susitikimų vietose.
3.1.8.	Bendrasis principas – esant abejonių dėl leistino Informacinio/IRT turto naudojimo, darbuotojas turi pasitarti su tiesioginiu vadovu, o Trečioji šalis su Sutarties / susitarimo savininku.
3.1.9.	Bendrasis principas – nesilaikant šios Politikos bus taikomos drausminės ir materialinės nuobaudos arba bus nutraukta darbo sutartis / susitarimas su Trečiąja šalimi.
3.1.9.1.	Bendrasis principas – jei Darbuotojas / Trečioji šalis susiduria su toliau nurodytais klausimais, Darbuotojas / Trečioji šalis turi laikytis ISCP nurodytų reikalavimų:
3.1.9.1.1.	ICS valdymas;
3.1.9.1.2.	Personalo valdymas;
3.1.9.1.3.	ICS strategija;
3.1.9.1.4.	Trečiųjų šalių teikėjų pasitelkimas;
3.1.9.1.5.	Informacinioos ir IRT turto naudojimas ir valdymas;
3.1.9.1.6.	ICS rizikos valdymas;
3.1.9.1.7.	Loginis saugumas;
3.1.9.1.8.	Pareigų atskyrimas;
3.1.9.1.9.	IRT aplinkų atskyrimas;
3.1.9.1.10.	IRT operacijų saugumas;
3.1.9.1.11.	ICS stebėsena;
3.1.9.1.12.	ICS peržiūra, vertinimas ir testavimas;
3.1.9.1.13.	Mokymasis ir tobulėjimas;
3.1.9.1.14.	IRT operacijų valdymas;
3.1.9.1.15.	ICS incidentų valdymas;
3.1.9.1.16.	IRT projektų valdymas;
3.1.9.1.17.	IRT įsigijimas ir vystymas;.
3.1.9.1.18.	Pokyčių kontrolė.
3.2.	**Informacinio turto naudojimas, perdavimas ir tvarkymas**
3.2.1.	Saugomas informacinis turtas turi būti naudojamas laikantis Konfidencialios informacijos saugojimo ir supažindinimo su ja tvarkos (EE filiale – Komercinę paslaptį sudarančios informacijos sąrašu).
3.2.2.	Asmens (saugomi) informacija turi būti naudojami pagal Asmens duomenų teisinės apsaugos tvarką (Asmens duomenų tvarkymo politiką EE filiale).
3.2.3.	Bet koks keitimasis informacija (įskaitant per socialinius tinklus) turi atitikti Reputacijos ir išorės komunikacijos politiką.
3.2.4.	Be Savininko leidimo draudžiama atskleisti Bendrovės / Grupės informacinį turtą Trečiosioms šalims.
3.2.5.	Dirbdamas su saugomu Informaciniu turtu kompiuteryje (įskaitant išmaniuosius telefonus, planšetinius kompiuterius ir kitus ICT) ar perduodamas saugomą informacinį turtą telefonu, darbuotojas / Trečioji šalis privalo imtis priemonių, kad ekrane rodomos informacijos negalėtų matyti ar girdėti neįgaliotas asmuo.
3.2.6.	Darbuotojai / Trečioji šalis, kuriems suteikta prieiga prie Asmens informacijos, privalo užtikrinti, kad jais naudojasi atsižvelgdami į konkrečius veiklos, pvz., atnaujinimas, pretenzijos nagrinėjimas ir pan., reikalavimus.
3.2.7.	Draudžiama saugoti ar tvarkyti Bendrovės / Grupės informacinį turtą neautorizuotuose IRT. PASTABA: Asmeniniai IRT nėra priskiriami autorizuotiems IRT.
3.2.8.	Draudžiama saugoti ar tvarkyti Bendrovės / Grupės informacinį turtą ilgiau, nei tai yra būtina.
3.2.9.	Asmeninės / viešosios internetinės failų saugyklos neturi būti naudojamos Bendrovės / Grupės informaciniam turtui saugoti ar persiųsti, taip pat Bendrovės / Grupės verslo reikalais.
3.2.10.	Draudžiama palikti balso pranešimus, kuriuose minima saugotina informacija, telefono atsakikliuose. Draudžiama siųsti teksto pranešimus, kuriuose minima saugotina informacija tam autorizacijos neturinčioms šalims.
3.2.11.	Informacinis turtas gali būti perduodami įvairiais IRT, įskaitant el. paštu, balso paštu, faksu, vaizdo priemonėmis ir pan. Darbuotojai / Trečiosios šalys turi užtikrinti, kad perduodant informacinį turtą būtų laikomasi šios Politikos.
3.2.12.	Bendrovės IRT gali būti naudojami tik su darbu susijusios informacijos saugojimui, apdorojimui ir perdavimui.
3.3.	**El. pašto naudojimas**

3.3.1.	Bendrovės el. paštas skirtas naudoti tik darbo reikalais; draudžiama jį naudoti asmeniniais tikslais.
3.3.2.	Visas saugomas informacinis turtas, perduodamas el. paštu, turi būti užšifruotas Bendrovės nustatytomis priemonėmis: suglaudintas (zip glaudinimas) ir apsaugotas slaptažodžiu ar perduodamas per „Cryptshare“ tarnybą.
3.3.3.	Asmenines el. pašto dėžutes draudžiama naudoti Bendrovės informaciniam turtui saugoti ar perduoti, taip pat naudoti verslo tikslais.
3.3.4.	El. laiškai neturi būti automatiškai persiunčiami į išorės ar vidaus el. pašto paskyras. Siekdama užtikrinti veiklos tęstinumą ir tik ribotam laikui Bendrovė gali persiųsti darbuotojo / Trečiosios šalies, su kuriais nutraukti darbo santykiai, el. pašto srautą tiesioginiam vadovui / sutarties savininkui.
3.3.5.	Gavęs įtartino ar draudžiamo turinio el. laišką darbuotojas (ar Trečioji šalis, besinaudojanti Bendrovės / Grupės IRT) turi skubiai apie tai pranešti bendrovėje naudojamomis priemonėmis (pvz., Hoxhunt ar analogiškomis).
3.4.	**Priimtinas IRT (įskaitant išmaniuosius telefonus ar kitas mobiliąsias IRT) naudojimas**
3.4.1.	Darbo reikalais leidžiama naudoti tik Bendrovės autorizuotą IRT turtą. Draudžiama darbo reikalais naudotis Bendrovės neautorizuotais IRT.
3.4.2.	IRT turi būti naudojami pagal šioje Politikoje nustatytas taisykles, įskaitant Savininko, ITDEP ir gamintojo instrukcijas.
3.4.3.	Draudžiama prie Bendrovės IRT, įskaitant kompiuterius, Tinklus (netaikoma Svečio tinklams), įrangą, saugojimo laikmenas ir pan., jungti asmeninius IRT. Draudžiama prie Bendrovės tinklų ar IRT jungti Trečiosios šalies (neautorizuotus ITDEP) IRT (netaikoma Svečio tinklams).
3.4.4.	Draudžiama leisti naudotis Bendrovės IRT bet kokiam kitam asmeniui (išskyrus autorizuotas Trečiąsias šalis).
3.4.5.	Draudžiama naudojantis Bendrovės IRT peržiūrėti ir naudoti su darbu nesusijusias medijas, informaciją ar turinį.
3.4.6.	Naudojantis bendrovės IRT privalu užtikrinti informacijos konfidencialumą. (Rekomenduojama nesinaudoti Bendrovės IRT žmonių susibūrimo vietose, pavyzdžiui, oro uostuose, traukiniuose, kavinėse ir pan. Jei nėra jokios kitos galimybės, užtikrinkite, kad jus supantys žmonės negalėtų matyti jūsų ekrane rodomos informacijos, nugirsti su verslu susijusių pokalbių ar gauti prieigą prie bet kokios su verslu susijusios informacijos. PASTABA: Mobiliųjų įrenginių (įskaitant nešiojamus kompiuterius) naudojimas privalo atitikti šios Politikos reikalavimus kurie yra taikomi visų IRT naudojimui. Atveju kai mobilus įrenginys (įskaitant nešiojamus kompiuterius) buvo pamestas (ar prarastas) jo Savininkas privalo nedelsiant apie tai pranešti vadovaudamasis Incidentų valdymo ir pranešimo apie juos nuostatomis (3.11).
3.5.	**Informacinio/IRT turto grąžinimas**
3.5.1.	Baigus galioti ar pasikeitus darbo sutarčiai ar susitarimui, Personalo nariai / Trečiosios šalys privalo grąžinti visą jų turimą ir nebenaudojamą darbui Bendrovės Informacinį/IRT turtą. Informacinio/IRT turto grąžinimas turi būti suderintas su darbuotojo tiesioginiu vadovu, sutarties su Trečiąja šalimi savininku ir ITDEP atstovu (arba IT paslaugų teikėjų EE filiale). Pasikeitus sutarčiai, darbuotojas / Trečioji šalis privalo grąžinti tik tą Informacinį/IRT turtą, kuris daugiau nėra būtinas tiesioginėms pareigoms vykdyti.
3.6.	**Programinės įrangos diegimo apribojimas**
3.6.1.	Leidžiama naudoti tik autorizuotą programinę įrangą. Draudžiama savarankiškai diegti, įkelti ar paleisti neautorizuotą programinę įrangą.
3.6.2.	Draudžiama pašalinti ar modifikuoti Bendrovės / Grupės suteiktą programinę įrangą.
3.7.	**Nuotolinis darbas**
3.7.1.	Nuotolinis darbas reiškia visas darbo ne biure formas, įskaitant netradicines darbo aplinkas, pavyzdžiui, darbas naudojantis nuotolinėmis telekomunikacijos priemonėmis, „lanksti darbo vieta“, nuotolinio ar virtualaus darbo aplinkos. Dirbdamas nuotoliniu būdu, darbuotojas / Trečioji šalis yra atsakingi už šioje Politikoje nustatytų reikalavimų laikymąsi. Jei dirba nuotoliniu būdu, Darbuotojai / Trečiosios šalys privalo užtikrinti nuotolinio darbo atitiktį Fizinio saugumo politikos reikalavimams.
3.7.2.	Dirbti nuotoliniu būdu leidžiama tik naudojantis autorizuotomis Bendrovės / Grupės IRT ir tik autorizuotomis Tinklo priemonėmis – virtualaus privačiojo tinklo (VPN) ryšiu su Bendrovės tinklu.
3.7.3.	Dirbdamas nuotoliniu būdu darbuotojas / Trečioji šalis privalo vykdyti šioje Politikoje ir, jei taikytina, ICSP nustatytus reikalavimus.

3.7.4.	Darbuotojas / Trečioji šalis privalo laikytis reikalavimo, kad šeimos nariai ar draugai yra laikomi neautorizuotais subjektais ir neturi teisės naudoti, žinoti ar gauti prieigą prie Bendrovės / Grupės Informacinio/IRT turto.
3.7.5.	Personalui / Trečiosiomis šalims draudžiama bandyti iššifruoti Bendrovės virtualiojo privataus tinklo (VPN) srautą ar prijungti neautorizuotus IRT prie Bendrovės / Grupės IRT.
3.7.6.	Bendrovė draudžia dirbti nuotoliniu būdu naudojantis nesaugiais privačiais ir viešaisiais tinklais. Jungdamasis prie Bendrovės tinklų vartotojas privalo visada naudotis VPN ryšiu.
3.7.7.	Darbuotojams / Trečiosioms šalims draudžiama ardyti ar modifikuoti / taisyti Bendrovės / Grupės IRT. Draudžiama leisti kitiems asmenims konfigūruoti / taisyti neveikiančius IRT. Šią funkciją gali atlikti tik IT pagalbos tarnyba.
3.8.	**Prieigos prie Informacinio/IRT turto suteikimas**
3.8.1.	Jei darbuotojas / Trečioji šalis pageidauja naudoti Bendrovės / Grupės Informacinį/IRT turtą (sistemas, kompiuterius, paslaugas ir pan.), jiems turi būti suteikta prieiga (autorizacija prieiti) prie Informacinio/IRT turto, bei patvirtinti prieigos atributai ir teisės. Prieigos atributai yra Vartotojo ID, slaptažodis, kai įmanoma – antras autentiškumo patvirtinimo veiksnys (2FA), pvz., PIN kodas. Bendrovėje leidžiama naudoti ir biometrines žymas (pirštų atspaudus ar „Face ID“, pakeičiančius Vartotojo ID ir slaptažodį), jei tai neprieštarauja Bendrovės vidaus teisės aktams. Prieigos teisės apima leidimą pasinaudoti įvairiu Informaciniu/IRT turtu.
3.8.2.	Prieiga prie Bendrovės IRT 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“ ir “Mažiausių privilegijų” principų. Darbuotojam / Trečiosioms šalims turi būti pasiekiama tik tiek Informacijos, kiek būtina.
3.8.3.	Jei vartotojo paskyra nėra naudojama ilgiau kaip 90 dienų, tokia paskyra turi būti automatiškai sustabdoma. Ši nuostata negalioja bendrovės klientų paskyroms.
3.8.4.	Naudojimasis IRT administratoriaus prieiga ir teisėmis yra griežtai ribojamas ir kontroliuojamas. Administratoriaus teisės suteikiamos tik kai tai yra būtina tiesioginėms pareigoms vykdyti. Vartotojo ID, skirti atlikti administratoriaus funkcijas ir įprastas užduotis, privalo būti skirtingi (negali būti naudojama ta pati paskyra).
3.8.5.	Kiekviena nevardinė techninė ir sisteminė paskyra turi turėti priskirtus techninį arba veiklos administratorius.
3.8.6.	Draudžiama atskleisti Vartotojo ID ir (arba) slaptažodį / 2FA kitam asmeniui / šaliai ar naudoti kito subjekto Vartotojo ID ir slaptažodį / 2FA.
3.8.7.	Slaptažodžių (įskaitant PIN kodus) saugumas:
3.8.7.1.	Draudžiama naudoti vienodus slaptažodžius, 2FA, / PIN kodus (ar kitus kredencialus) skirtinguose IRT (Bendrovės ar asmeniniuose).
3.8.7.2.	Draudžiama atskleisti slaptažodžius / 2FA / PIN kodus kitiems subjektams, įskaitant Bendrovės / Grupės Darbuotojams.
3.8.7.3.	Slaptažodžius / 2FA / PIN kodus būtina įsiminti. Draudžiama juos laikyti užrašytus (elektroninėje ar popierinėje laikmenoje).
3.8.7.4.	Laikinuosius slaptažodžius / 2FA / PIN kodus privaloma pakeisti po pirmojo prisijungimo.
3.8.7.5.	Mažiausias privalomas slaptažodžių sudėtingumas: Vartotojo paskyros slaptažodžius turi sudaryti bent 14 simbolių. Jei naudojama 2FA autentifikavimą, slaptažodį turi sudaryti bent 10 simbolių. Administratoriaus paskyros slaptažodžius turi sudaryti bent 16 simbolių. Sisteminės ir techninės paskyros slaptažodžio ilgis turi sudaryti ne mažiau negu 20 simbolių. Slaptažodžius turi būti sudaryti bent iš trijų simbolių tipų nurodytų toliau - didžiosios raidės / mažosios raidės, skaičiai, specialieji simboliai. Slaptažodžių negali sudaryti lengvai atspėjami žodžiai ar sekos (pvz., P@ssword1, V!lnius2018, qwerty, ABC123!@# ir t. t.);
3.8.7.6.	Mažiausias PIN kodų sudėtingumas yra 6 simbolių unikali kombinacija.
3.8.7.7.	Slaptažodžius / PIN kodus reikia keisti kas 3 mėnesius (kur yra techninės galimybės, Vartotojas bus paragintas tai atlikti arba Vartotojas turi pats prisiminti, kad būtina pakeisti slaptažodį / PIN kodą rankiniu būdu). Slaptažodis / PIN kodas negali kartotis paskutinius 10 keitimų iš eilės. Techninės paskyros slaptažodžius esant galimybei būtina keisti kas 12 mėnesių, o turint įtarimų kad jos prisijungimo rekvizitai tapo žinomi neautorizuotiems asmenims, slaptažodžio keitimas turi būti atliktas nedelsiant. Sisteminės paskyros slaptažodis privalomai turi būti pakeistas pirmojo konfigūravimo arba instaliavimo metu ir esant galimybei keičiamas bent kas 24 mėn.

3.8.7.8.	Įvedami slaptažodžiai / PIN kodai neturi būti matomi kitiems asmenims.
3.8.7.9.	Vartotojui klaidingai suvedus slaptažodį 5 kartus, paskyra turi būti blokuojama. Esant techninėms galimybėm, pakartotinai gali būti leidžiamas pakartotinis bandymas autentifikuotis ne anksčiau negu po 5 minučių.
3.8.7.10.	Jei autentifikavimo priemonės leidžia vartotojams likti prisijungusiems, rekomenduojama, jei tai leidžia techninės galimybės, periodiškai vykdyti pakartotinį autentifikavimą tiek aktyviai naudojant, tiek po neveikos laikotarpio. Rekomenduojami vartotojų sesijos trukmės valdymo periodai (laikas gali būti koreguojamas, jei laiko keitimas yra pagrįstas verslo logikai):
3.8.7.10.1.	Vartotojo nepertraukiamo darbo trukmė turėtų būti 12 valandų, po to turėtų būti reikalaujama pakartotinio autentiškumo patvirtinimo.
3.8.7.10.2.	Jei sesija neaktyvi ilgiau nei 30 minučių, sesija turi būti nutraukta ir reikalaujamas pakartotinis autentifikavimas.
3.8.7.10.3.	Kompiuterių darbo vietų darbalaukio užraktas turėtų įsijungti po 5 minučių neveikimo.
3.9.	**Švaraus stalo ir švaraus ekrano principas**
3.9.1.	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.	Be priežiūros negalima palikti darbo vietoje jokių I/D, kurie gali būti pasiekiami be slaptažodžio ar kito informacijos apsaugos mechanizmo.
3.9.3.	Saugomus I/D reikia visada tvarkyti laikantis I/D klasifikacijos, teisinių / sutartinių reikalavimų, taip pat šios Politikos reikalavimų, įskaitant I/D Savininkų nustatytus reikalavimus.
3.10.	**Vartotojų veiklos stebėsena**
3.10.1.	Siekdama vykdyti ICSP, Bendrovės / Grupės ar Lietuvos Respublikos teisinius reikalavimus (EE padalinyje – Estijos Respublikos teisinius reikalavimus), Bendrovė stebi Personalo / Trečiųjų šalių veiklą Bendrovei / Grupei priklausančiuose IRT.
3.11.	**Incidentų valdymas ir informavimas apie juos**
3.11.1.	Darbuotojai / Trečiosios šalys, pastebėjusios ar įtarusios ICS incidentą, privalo nedelsdamos apie tai informuoti IT pagalbos tarnybą.
3.11.2.	Darbuotojai / Trečiosios šalys, sužinojusios apie galimą ICS pažeidžiamumą, privalo nedelsdamos apie tai informuoti IT pagalbos tarnybą.
3.11.3.	Rizikos valdymo funkcija turi būti informuojama apie visus šios Politikos pažeidimus pagal Operacinės rizikos valdymo politikos reikalavimus.
3.12.	**Informuotumo didinimas ir mokymas ICS klausimais**
3.12.1.	Darbuotojai ir, kur taikytina, Trečiosios šalys turi dalyvauti visoje informuotumo didinimo ir mokymo ICS klausimais veikloje, kad užtikrintų reikiamą įgūdžių ir žinių ICS srityje lygį.
4.	**Pareigos ir atsakomybė**
4.1.	Bendrovės darbuotojai atsakingi už šios Politikos įgyvendinimą savo atsakomybių ribose / srityse.
4.2.	Politikos Savininkas (CSM) yra atsakingas už Politikos turinio atnaujinimą, reikalavimų aktualumą ir keliamos rizikos mažinimą .
4.3.	IRT ir Saugumo Rizikų Pareigūnas yra atsakingas vykdyti Politikos rengimo ir įgyvendinimo priežiūrą.
4.4.	Darbuotojai / Trečiosios šalys yra atsakingi informuoti apie verslo sritims, kurioms taikoma Politika, keliamą riziką ir Politikos pažeidimus Politikos savininką ar IRT ir Saugumo Rizikų Pareigūną ir Rizikos valdymo funkciją.

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.