Norminis vidaus teisės akto pavadinimas	**AB „Ignitis grupė“ įmonių grupės informacijos saugos politika**
Proceso pavadinimas	Informacijos saugos valdymo
Proceso savininkas (padalinys)	UAB „Ignitis grupės paslaugų centras“ Skaitmeninė sauga
Tvirtinančioji įmonė	AB „Ignitis grupė“
Tvirtinančio asmens pareigybė/ organas	AB „Ignitis grupė“ valdyba
Įsigaliojimo data	2024-10-01

AB „IGNITIS GRUPĖ“ ĮMONIŲ GRUPĖS INFORMACIJOS SAUGOS POLITIKA

1. TIKSLAS IR TAIKYMO APIMTIS

1.1. Politikos tikslas – nustatyti Grupės Informacijos saugos užtikrinimo kryptis ir principus, Grupės Informacijos gavėjų ir naudotojų pareigas, siekiant užtikrinti Grupės valdomos informacijos apsaugą nuo jos neteisėto gavimo, naudojimo ir atskleidimo; taip pat užtikrinti Grupės informacijos vientisumą ir prieinamumą bei suvaldyti Informacijos saugos rizikas Grupėje iki toleruojamo lygio.

1.2. Politika apima visą Grupės informaciją, nepriklausomai nuo jos formos, pobūdžio, įvedamą, perduodamą ar saugomą Grupės Informacinėse sistemose ir (ar) Debesijos paslaugų sistemose. Politika taip pat apima Darbuotojų naudojamus Grupės išduodamus įrenginius arba prijungtus prie Grupės Informacinių sistemų ir (ar) Debesijos paslaugų sistemų, įskaitant, bet neapsiribojant, mobiliuosius telefonus, planšetinius kompiuterius, nešiojamuosius ir stacionarius kompiuterius.

1.3. Politika taikoma visoms Grupės Įmonėms ir privaloma visiems Grupės Įmonių Darbuotojams ir Paslaugų teikėjams.

1.4. Grupės Įmonės, kurios registruotos ir veikia užsienio šalyse, šią Politiką taiko tiek, kiek tai neprieštarauja tų šalių teisės aktams.

2. SĄVOKOS

2.1. Bendrinės sąvokos aprašomos Sąvokų žodyne: Bendrovė, Darbuotojas, Debesija, Duomenys, Grupė, Grupės paslaugų centras, Informacija, Informacinis turtas, Informacinio turto savininkai, Informacijos sauga, IT, Įmonė, Konfidenciali informacija, Kritinis procesas, Nuotolinė darbo vieta, OT, Paskyra, Prieigos teisės, Toleruojamas rizikos lygis, Užklausų valdymo sistema, Vidaus teisės aktas.

2.2. **Informacinė sistema** – IT arba OT sistema.

2.3. **Išorinė laikmena** – bet kokios rūšies (elektroninė, magnetinė ar optinė) duomenų laikmena, kuri nėra Įrenginio dalis (pvz., USB raktai, išoriniai kietieji diskai, CD, DVD ir kt.).

2.4. **Įrenginys** – telefonas ir (ar) kompiuteris (planšetinis, nešiojamasis, stacionarusis ar kt.) ir (ar) jų priedai.

2.5. **Kolegialus organas** -– Bendrovės ir (ar) Įmonių steigimo dokumentuose nurodytas kolegialus valdymo organas – valdyba, ir (ar) priežiūros organas – stebėtojų taryba.

2.6. **Mobilusis įrenginys** – nešiojamasis kompiuteris, planšetinis kompiuteris, mobilusis telefonas.

2.7. **Paslaugų teikėjas** – Trečioji šalis, teikianti paslaugas Įmonėms.

2.8. **Politika** – AB „Ignitis grupė“ įmonių grupės informacijos saugos politika, šis dokumentas.

2.9. **Trečioji šalis** – fizinis asmuo, kuris nėra Grupės Darbuotojas ar Kolegialaus organo ar Bendrovės komiteto narys, ar juridinis asmuo, kuris nepriklauso Grupei.

3. BENDROSIOS NUOSTATOS

3.1. Grupės Informacija yra vertinga Grupės Įmonių turto dalis. Jos praradimas, neteisėtas gavimas,pakeitimas ar atskleidimas gali daryti neigiamą įtaką Grupės ir (ar) Įmonių strateginių tikslų pasiekimui bei konkurencingumui, įvaizdžiui ir reputacijai.

3.2. Grupės Įmonės vykdo veiklą Lietuvos Respublikos nacionaliniam saugumui svarbiame ūkio sektoriuje, todėl Informacijos konfidencialumo, teisingumo, integralumo ir prieinamumo užtikrinimas yra ypatingai svarbus. Siekdama apsaugoti klientų, partnerių, rangovų ir Grupės Informaciją bei Informacines sistemas, Grupė skiria didelį dėmesį Informacijos ir Informacinių sistemų saugai, taip pat įdarbinimo ir darbo santykių nutraukimo ir (ar) pabaigos procesams, Darbuotojų kompetencijų kėlimui dirbant Grupėje, Trečiųjų šalių ir (ar) jų darbuotojų kompetencijų ir patikimumo įvertinimui.

3.3. Šios Politikos nuostatos taikomos atsižvelgiant į Lietuvos Respublikos teisės aktų ar atitinkamų užsienio valstybės teisės aktų reikalavimus. Jei yra teisės aktų ir Politikos neatitikimų, Politika taikoma tiek, kiek neprieštarauja teisės aktams. Taikant Politiką taip pat vadovaujamasi tarptautiniais standartais ir (ar) gerosiomis praktikomis, tarp jų:

3.3.1. Tarptautinis standartas ISO/IEC 27001 „*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*“;

3.3.2. Lietuvos standartas LST EN ISO/IEC 27002 „*Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės (ISO/IEC 27002:2022)*“, kuris yra perimtas Europos standartas EN ISO/IEC 27002:2022 „*Information security, cybersecurity and privacy protection – Information security controls“;*

3.3.3. Tarptautinis standartas ISO/IEC 27017 „*Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*“;

3.3.4. Tarptautinis standartas ISO/IEC 27018 „*Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*“;

3.3.5. Tarptautinis standartas IEC 62443 „*Industrial communication networks – Network and system security*“.

3.4. Grupės Įmonėms Informacijos saugos paslaugas teikiantis Grupės paslaugų centras turi būti sertifikuotas pagal šios Politikos 3.3.1 papunktyje nurodytą tarptautinį standartą ir turi užtikrinti, kad paslaugoms teikti pasitelkti Tretieji asmenys laikysis teisės aktų ir šios Politikos reikalavimų, taip pat savo veikloje vadovausis tarptautiniais standartais ir (ar) gerosiomis praktikomis.

3.5. Siekiant šios Politikos tikslų, Grupėje veikia reagavimo į kibernetinius incidentus komanda „Ignitis CERT“, kuri savo veikloje vadovaujasi tarptautiniais reagavimo į kibernetinius incidentus (toliau CERT/CSIRT) komandų principais ir standartais, dalyvauja pasaulines CERT/CSIRT komandas vienijančiose organizacijose, tarp jų TF-CSIRT, bei palaiko akredituoto nario TF-CSIRT organizacijoje statusą.

3.6. Šios Politikos nuostatos detalizuojamos Grupės ir (ar) Bendrovės, ir (ar) Įmonės vidaus teisės aktuose, kurie privalo neprieštarauti šiai Politikai.

3.7. Visas Politikos nuostatų taikymo išimtis tvirtina Grupės paslaugų centro skaitmeninės saugos vadovas Užklausų valdymo sistemoje arba elektroninio ryšio priemonėmis, užtikrinant atsekamumą.

4. INFORMACIJOS SAUGOS UŽTIKRINIMO KRYPTYS IR PRINCIPAI

4.1. **Mokymai ir švietimas.** Grupėje vystoma Informacijos saugos kultūra, kad Darbuotojai tinkamai suvoktų Informacijos ir jos saugos svarbą, neteisėto Informacijos gavimo, pakeitimo, naudojimo ir atskleidimo galimą neigiamą poveikį Grupės veiklai, Įmonėms keliamų tikslų įgyvendinimui. Siekiama nuolatos didinti Darbuotojų atsparumą Informacijos saugos grėsmėms periodiškai organizuojant mokymus, tikrinant Darbuotojų žinias, vykdant nuolatinę komunikaciją apie Grupei aktualias Informacijos saugos grėsmes ir priemones, leidžiančias išvengti Informacijos saugos incidentų. Be to, Grupės Įmonių deleguoti Darbuotojai dalyvauja Šiaurės Atlanto sutarties organizacijos (NATO) ir (ar) Lietuvos Respublikos institucijų organizuojamose kibernetinio saugumo pratybose.

4.2. **Aiški savininkystė.** Didžiausią vertę turintis Informacinis turtas, tarp jo ir Įmonių konfidenciali informacija ir komercinės (gamybinės) paslaptys, turi būti identifikuotas bei paskirti už jį atsakingi Informacinio turto savininkai. Taip pat Grupėje turi būti paskirti IT paslaugų ir sistemų, OT įrenginių savininkai, turintys sprendimų teisę ir valdantys reikalingus išteklius bei atsakingi už tinkamą Informacijos saugos valdymą.

4.3. **Rizikos valdymas.** Grupės Informacijos saugos valdymo sistema yra pagrįsta rizikų identifikavimu, vertinimu ir stebėsena. Grupės Kritinių procesų, Informacinių sistemų Informacijos saugos grėsmių rizikos turi būti vertinamos periodiškai, taip pat ir atsiradus poreikiui (pavyzdžiui, kuriant naujas ar keičiant esamas Informacines sistemas, verslo procesus). Identifikuota rizika turi būti mažinama iki Toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstas, kainos ir efektyvumo atžvilgiu subalansuotas bei tarptautinius Informacijos saugą reglamentuojančius standartus atitinkančias Informacijos saugos priemones. Vertinant Informacijos saugos rizikas, taip pat turi būti įvertintos fizinės ir gamtinės kilmės grėsmės.

4.4. **Atitiktis**. Grupėje įgyvendinami teisės aktuose įtvirtinti Informacijos saugos reikalavimai, atsižvelgiant į šalies, kurioje Įmonė vykdo veiklą, reguliavimą, taip pat įgyvendinami Įmonių sutartiniai įsipareigojimai ir kiti įsipareigojimai, taikant rizikos vertinimu pagrįstas Informacijos saugos priemones.

4.5. **Santykiai su Trečiosiomis šalimis.** Informacijos, kuri teikiama ir (ar) gaunama vykdant ikisutartinius ir (ar) sutartinius santykius su Trečiosiomis šalimis, saugumas turi būti užtikrintas per visą ikisutartinių ir (ar) sutartinių santykių ir (ar) įsipareigojimų galiojimo laikotarpį ar jiems pasibaigus, įskaitant, bet tuo neapsiribojant, į susitarimus ir sutartis įtraukiant Informacijos saugos nuostatas, įpareigojančias Informacijos gavėjus užtikrinti ne mažesnį Informacijos saugos lygį nei taikomas Grupėje. Grupė bendradarbiauja su kibernetinio saugumo politiką formuojančiomis ir įgyvendinančiomis Lietuvos Respublikos institucijomis, dalyvauja profesiniuose forumuose, dalinasi su Informacijos sauga bei jos grėsmėmis susijusia informacija bei gerąja Informacijos saugos praktika su kitomis įmonėmis ir organizacijomis.

4.6. **Grėsmių žvalgyba, incidentų ir pažeidžiamumų valdymas.** Grupėje nuolat vykdoma grėsmių žvalgyba, renkant ir analizuojant informaciją, susijusią su Informacijos saugos grėsmėmis. Informacijos saugos incidentai, įvykiai bei pažeidžiamumai sistemingai ir nuosekliai identifikuojami, vertinami ir valdomi, užtikrinant tinkamą reagavimą, suvaldymą ir priemonių numatymą, siekiant išvengti incidentų pasikartojimo ar pažeidžiamumų išnaudojimo.

4.7. **Informacijos sauga projektų ir pokyčių valdyme.** Informacijos sauga turi būti įtraukiama į visas pokyčių projektų vykdymo fazes. Prieš inicijuojant naujus Informacinių sistemų, Debesijos paslaugų sistemų projektus ar planuojant esminius pokyčius, turi būti įvertintos galimos Informacijos saugos rizikos ir parenkamos atitinkamos Informacijos saugos priemonės.

5. INFORMACIJOS SAUGOS UŽTIKRINIMO DALYVIAI IR JŲ PAREIGOS

5.1. Visi Grupės Informacijos saugos dalyviai (subjektai, kurie yra įtraukti į Informacijos saugos valdymo procesus) turi pareigą laikytis šios Politikos, teisės aktuose įtvirtintų Informacijos saugos reikalavimų bei ikisutartinių ir (ar) sutartinių įsipareigojimų.

5.2. **Bendrovės valdyba** tvirtina šią Politiką, nustato Informacijos saugos užtikrinimo kryptis, tikslus, siekius ir principus Grupėje.

5.3. **Darbuotojai** užtikrina Informacijos saugumą kasdienėje veikloje vykdydami darbo funkcijas, priimdami sprendimus, identifikuojant, vertinant ir stebint Informacijos saugos rizikas bei parenkant priemones joms suvaldyti ir juos derinant su Informacijos saugos reikalavimais. Darbuotojai atsako už Informacijos saugos reikalavimų laikymąsi ir saugų jiems patikėto arba jiems žinomo Informacinio turto naudojimą.

5.4. **Įmonių vadovai** užtikrina, kad informacijos saugos reikalavimai būtų integruoti į veiklos planavimo procesus bei Informacijos saugos rizikos klausimus laiko neatsiejama Įmonių veiklos procesų dalimi, skiria tinkamą dėmesį ir išteklius Informacijos saugos užtikrinimui ir identifikuotų rizikų valdymui.

5.5. **Grupės paslaugų centro Skaitmeninės saugos padalinys** formuoja Grupės Informacijos saugos strategiją, organizuoja Grupės Informacijos saugos rizikų identifikavimą, vertinimą ir valdymą iki Toleruojamo rizikos lygio, teikia pagalbą Įmonėms valdant riziką, organizuoja mokymus darbuotojams, kontroliuoja Informacijos saugą reglamentuojančių Grupės vidaus teisės aktų poreikį, pakankamumą ir įgyvendinimą.

5.6. **Paslaugų teikėjai** užtikrina, kad jų infrastruktūra ir procesai atitiktų jiems keliamus Informacijos saugos reikalavimus, atsako už Informacijos saugos reikalavimų laikymąsi ir saugų Grupės Informacinio turto naudojimą.

5.7. **Kitos suinteresuotos šalys** – asmenys, turintys interesų ar teisių, susijusių su Informacijos sauga, tarp jų, Lietuvos Respublika, Bendrovės ir (ar) Įmonių akcininkai, Grupės Įmonių klientai, valstybių, kuriose veikia Grupės Įmonės, gyventojai, prekes ir paslaugas Grupės Įmonėms teikiantys asmenys ir kitos Trečiosios šalys.

6. INFORMACINIO TURTO VALDYMAS

6.1. Visa ne vieša Informacija yra Grupės nuosavybė, kurią privalo saugoti Darbuotojai ir Paslaugų teikėjai.

6.2. Visa Grupės Informacija pagal svarbą, galimos žalos ją atskleidus ar praradus dydį yra klasifikuojama į klases ir žymima žymomis:

6.2.1. Viešo naudojimo informacija (nežymima);
6.2.2. Vidaus naudojimo informacija (žymima žyma „VIDAUS NAUDOJIMO“);
6.2.3. Konfidenciali informacija:
6.2.3.1. išorės gavėjams (žymima žyma „KONFIDENCIALU“);
6.2.3.2. vidaus naudojimo (žymima žyma „KONFIDENCIALU“);
6.2.4. Griežtai konfidenciali informacija, skirta tik konkretiems gavėjams (žymima žyma „GRIEŽTAI KONFIDENCIALU“).
6.3. Žemiausia klasė yra Viešo naudojimo, aukščiausia (labiausiai saugoma) – Griežtai konfidenciali informacija.
6.4. Kiekviena Grupės Įmonė privalo patvirtinti Konfidencialios informacijos ir komercinių (gamybinių) paslapčių sąrašą, parengtą pagal Bendrovės valdybos patvirtintą pavyzdinį Konfidencialios informacijos ir komercinių (gamybinių) paslapčių sąrašą. Šiuose sąrašuose nurodytai Informacijai suteikiamas Griežtai konfidencialios arba Konfidencialios informacijos statusas.
6.5. Grupės Informacijos naudojimui, perdavimui ir valdymui turi būti taikomos saugos priemonės, numatytos Grupės informacijos konfidencialumo užtikrinimo standarte.
6.6. Grupės asmens duomenų apsaugos priemonės ir atsakomybės nustatytos Grupės asmens duomenų apsaugos politikoje ir susijusiuose teisės aktuose.

7. INFORMACIJOS SAUGOS PRIEMONĖS IR ĮSIPAREIGOJIMAI

7.1. Grupėje diegiamos inovatyviais saugos sprendimais paremtos ir identifikuotai rizikai proporcingos organizacinės ir techninės Informacijos saugos priemonės. Įvertinus galimus rizikos veiksnius Grupės Informacijai, taikomos detekcinės, prevencinės ir korekcinės rizikos valdymo priemonės.
7.2. Grupės Informacijos saugos valdymo sistemą sudaro šios organizacinės ir techninės priemonės (bet neapsiribojant):

7.2.1. **Prieigos teisių valdymas:**

7.2.1.1. Informacinio turto savininko sprendimu Prieigos teisės prie Informacinio turto Grupėje suteikiamos vadovaujantis principu „būtina žinoti“;
7.2.1.2. Grupės valdomų Informacinių sistemų ir Debesijos paslaugų sistemų, operacinių sistemų, duomenų bazių paskyros, įskaitant prieigą prie programinės įrangos kodo, turi būti valdomos centralizuotai per Užklausų valdymo sistemą;
7.2.1.3. Informacinio turto savininkai turi ne rečiau kaip kartą per metus peržiūrėti prie Informacinio turto suteiktas Prieigos teises, užtikrinant, kad jos yra suteiktos vadovaujantis principu „*būtina žinoti*“, o nereikalingos – nedelsiant naikinamos;
7.2.1.4. Prieigai prie Informacinių sistemų ir Debesijos paslaugų sistemų naudojamos saugios autentifikavimo priemonės;
7.2.1.5. Suteikiant Prieigas prie Informacinio turto Trečiosios šalims, turi būti gaunamas Trečiųjų šalių patvirtinimas, kad Prieigos bus naudojamos vadovaujantis šia Politika ir kitais Informacijos saugos reikalavimais, tik nurodytu tikslu, apimtimi ir būdais bei numatyta atsakomybė už nurodyto įsipareigojimo pažeidimą.

7.2.2. Duomenų perdavimo tinklų sauga:

7.2.2.1. Duomenų perdavimo tinklų perimetro sauga užtikrinama naudojant ugniasienes ir vykdant nuolatinę stebėseną tarp Grupės vidinio tinklo ir viešųjų ryšių tinklo (interneto);
7.2.2.2. Grupėje turi būti užtikrinama, kad OT duomenų perdavimo tinklas būtų fiziškai atskirtas nuo IT duomenų perdavimo tinklo;
7.2.2.3. Grupės Duomenų perdavimo tinklas segmentuojamas į atskiras tinklo saugumo zonas, atsižvelgiant į Informacinių sistemų svarbą ir identifikuotas rizikas;
7.2.2.4. Grupės Informacinį turtą iš Nuotolinės darbo vietos galima pasiekti tik šifruotu ryšiu;
7.2.2.5. Duomenų perdavimo saugumo užtikrinimas vykdomas vadovaujantis Grupės IT vadovo patvirtintu Grupės IT / OT sistemų saugos užtikrinimo standartu.

7.2.3. Informacinių sistemų veiklos sauga:

7.2.3.1. Grupės Informacinėse sistemose turi būti naudojamos kenkėjiškos programinės įrangos ir (ar) veiklos aptikimo, užkardymo ir stebėjimo priemonės;
7.2.3.2. visų Informacinių sistemų, Duomenų perdavimo tinklo įrenginių ir Įrenginių saugos žurnaliniai įrašai, įskaitant operacinės sistemos, duomenų bazių, taikomųjų programų, Grupėje turi būti kaupiami centralizuotai.

7.2.4. Įrenginių sauga:

7.2.4.1. Įrenginiai turi atitikti Grupės vidaus teisės aktuose nustatytus saugos reikalavimus. Visų Grupės Įrenginių nustatymai yra valdomi Grupės IT funkcijos;

7.2.4.2. Darbuotojams suteikti Įrenginiai, elektroninis paštas, interneto resursai yra skiriami darbo funkcijoms vykdyti, o jų naudojimo asmeniniams tikslams sąlygos yra nustatomos Grupės ir (ar) Įmonės vidaus teisės aktais;

7.2.4.3. preziumuojama, kad Mobilieji įrenginiai yra dažnai naudojami nesaugiose aplinkose, jų skaitmeninės saugos rizika yra aukštesnė, todėl joms taikomos ne mažiau efektyvios saugos priemonės nei nuolatinėje darbo vietoje naudojamuose Įrenginiuose;

7.2.4.4. asmeninių Įrenginių, išskyrus mobiliųjų telefonų, naudojimas Grupės tinkle yra draudžiamas. Asmeniniai mobilieji telefonai gali būti naudojami Grupės tinkle Grupės vidaus teisės aktais nustatyta tvarka;

7.2.4.5. Grupės Informacija ir darbui skirtos programos mobiliuosiuose telefonuose ir planšetiniuose kompiuteriuose pasiekiamos tik naudojant Mobiliųjų įrenginių valdymo (angl. *Mobile Device Management, MDM*) sprendimą;

7.2.4.6. Grupės valdomų Debesijos paslaugų sistemos pasiekiamos tik iš Grupės valdomų Įrenginių. Išimtis gali būti taikoma Bendrovės ir Įmonių Kolegialių organų ar komitetų nariams.

7.2.5. Žmogiškasis faktorius:

7.2.5.1. Darbuotojai, Kolegialių organų ar komitetų nariai, Paslaugų teikėjai ir (ar) kitos Trečiosios šalys turi pareigą saugoti Grupės Informacinį turtą. Grupėje užtikrinama, kad raštiški įsipareigojimai dėl Konfidencialios informacijos saugojimo būtų įtraukti į darbo sutartis, sutartis, sudaromas su Paslaugų teikėjais, gaunami ikisutartiniuose santykiuose ar teikiant Informacinį turtą bet kokiu pagrindu Trečiosioms šalims;

7.2.5.2. prieš įdarbinant asmenis ar prieš sudarant sandorius su Trečiosiomis šalimis, turi būti atliekamas atitinkamai atrinktų kandidatų ir Trečiųjų šalių patikrinimas vadovaujantis Grupės vidaus teisės aktais;

7.2.5.3. Darbuotojams ir (ar) Kolegialių organų nariams yra suteikiamos tokios Prieigos teisės prie Informacinio turto, kokios yra būtinos jų funkcijoms atlikti ir tik susipažinus su Informacijos saugą reglamentuojančiais Grupės vidaus teisės aktais;

7.2.5.4. Darbuotojai periodiškai supažindinami su Grupės Informacijos saugą reglamentuojančiais teisės aktais. Grupėje ne rečiau kaip kartą per metus turi būti organizuojami darbuotojų Informacijos saugos žinių kėlimo mokymai, tikrinamos Darbuotojų atsparumo Informacijos saugos grėsmėms žinios ir įgūdžiai;

7.2.5.5. pasibaigus darbo ir (ar) civiliniams teisiniams santykiams, turi būti nedelsiant panaikintos suteiktos Prieigos teisės prie Informacinio turto.

7.2.6. Kriptografija:

7.2.6.1 Grupės Informacinio turto sauga turi būti užtikrinama naudojant visuotinai pripažintas saugias šifravimo priemones, kurioms keliami reikalavimai nustatomi Grupės vidaus teisės aktais;

7.2.6.1. Kriptografiniai raktai turi būti valdomi centralizuotai naudojant raktų valdymo sistemą;

7.2.6.2. šifravimo priemonės turi būti naudojamos visuose Mobiliuosiuose įrenginiuose, Išorinėse laikmenose ir Duomenų perdavimo tinkluose vadovaujantis Grupės vidaus teisės aktais;

7.2.6.3. siekiant identifikuoti kenkėjišką kodą, Duomenų perdavimo tinkluose šifruotas srautas gali būti dešifruotas analizės tikslams.

7.2.7. Fizinė sauga:

7.2.7.1. fizinė prieiga prie Grupės biurų ir kitų patalpų, kuriose saugomas Grupės Informacinis turtas, turi būti ribojama ir kontroliuojama, taikant prevencines ir detekcines kontrolės priemones;

7.2.7.2. fizinės saugos priemonės (pvz. švaraus stalo ir kompiuterio ekrano principai) taikomos tiek Įmonių biuruose, tiek Nuotolinėse darbo vietose;

7.2.7.3. užtikrinant Grupės fizinę saugą, turi būti vadovaujamasi ir kitais Grupės ir (ar) Įmonės vidaus teisės aktai, kurie reglamentuoja Grupės fizinę saugą.

7.2.8. Pažeidžiamumų valdymas:

7.2.8.1. Grupėje periodiškai turi būti vykdomas Informacinio turto IT ir OT komponentų pažeidžiamumų identifikavimas, vertinimas, stebėjimas ir šalinimas;

7.2.8.2. identifikuoti pažeidžiamumai turi būti klasifikuojami bei šalinami pagal prioritetus, atsižvelgiant į jų kritiškumo lygį.

7.2.9. Informacinių sistemų įsigijimas, kūrimas ir priežiūra:

7.2.9.1. naujai projektuojamos, kuriamos, įsigyjamos Informacinės sistemos bei esamų pokyčiai turi atitikti teisės aktuose nustatytus saugumo reikalavimus;

7.2.9.2. prieš pradedant naudoti Informacines sistemas ar jų dalis, turi būti atliekamas saugos vertinimas. Draudžiama naudoti saugumo reikalavimų neatitinkančias Informacines sistemas;

7.2.9.3. Grupėje naudojamos Informacinės sistemos ir jų komponentai (operacinės sistemos, duomenų bazių valdymo sistemos, kita susijusi programinė įranga) turi būti palaikomos gamintojo ir periodiškai atnaujinamos;

7.2.9.4. turi būti vertinamas ir planuojamas Grupėje naudojamų Informacinių sistemų gyvavimo ciklas;

7.2.9.5. veikloje nebenaudojamos Informacinės sistemos ar jų komponentai turi būti išjungti arba patalpinti į archyvą. Priimant sprendimą nenaudoti Informacinės sistemos, turi būti numatomos Informacinio turto saugojimo ar naikinimo priemonės, atsižvelgiant į teisės aktų reikalavimus.

7.2.10. Santykiai su Trečiosiomis šalimis:

7.2.10.1. Trečiosios šalys, teikiančios IT / OT paslaugas, Debesijos paslaugas Grupės Įmonėms ar tvarkančios Grupės Informacinį turtą, turi užtikrinti, kad jų infrastruktūra ir procesai atitinka jiems keliamus saugos reikalavimus;

7.2.10.2. Trečiosios šalys privalo pasirašyti konfidencialumo pasižadėjimą, susipažinti su šia Politika ir ja vadovautis;

7.2.10.3. Paslaugų teikėjams paslaugų teikimui būtinos prieigos prie Grupės Informacinio turto suteikiamos naudojant Užklausų valdymo sistemą;

7.2.10.4. turi būti užtikrintas Trečiųjų šalių, teikiančių IT / OT paslaugas, veiksmų stebėjimas ir registravimas;

7.2.10.5. Debesijos paslaugų teikimo sutartyse turi būti numatytos paslaugų pasiekiamumo, duomenų konfidencialumo nuostatos, Paslaugų teikėjo taikomos saugos kontrolės priemonės, atitiktis standartams ir teisės aktams, incidentų ir pažeidžiamumų valdymas, atsakomybės ir žalos atlyginimas, paslaugų sustabdymas ir paslaugų nutraukimas, užtikrinant Grupės duomenų perdavimą ar sunaikinimą.

7.2.11. Incidentų valdymas:

7.2.11.1. Darbuotojai, Kolegialių organų nariai, Paslaugų teikėjai ir kitos Trečiosios šalys turi pareigą pranešti apie pastebėtus Informacijos saugos incidentus;

7.2.11.2. Informacijos saugos incidentų valdymas turi apimti incidento identifikavimą, vertinimą, kategorizavimą ir prioritetizavimą, atsižvelgiant į incidento poveikį, stabdymą bei šalinimą;

7.2.11.3. patirtys, įgytos valdant incidentus, turi būti pritaikomos, siekiant išvengti incidentų ir (ar) ateityje sumažinti incidentų pasireiškimo tikimybę ir poveikį;

7.2.11.4. apie Grupėje vykstančius ir (ar) įvykusius Informacijos saugos incidentus turi būti informuojamos atitinkamos valstybės institucijos, gyventojai ir (ar) Paslaugų teikėjai teisės aktų nustatyta tvarka.

7.2.12. Rizikų valdymas ir veiklos tęstinumo užtikrinimas:

7.2.12.1. Periodinis Informacijos saugos rizikų identifikavimas, vertinimas ir stebėsena atliekama vadovaujantis Grupės rizikos valdymo politika;

7.2.12.2. Veiklos tęstinumas užtikrinamas vadovaujantis Grupės veiklos tęstinumo užtikrinimo politika.

7.2.13. Atitiktis ir auditas:

7.2.13.1. Grupės Įmonių Informacijos saugos įsipareigojimai Trečiosiomis šalimis, Grupės Įmonių vidaus bei išorės teisės aktų Informacijos saugos reikalavimai (atsižvelgiant į šalies, kurioje Grupės Įmonė vykdo veiklą) turi būti įgyvendinami taikant rizikos vertinimu pagrįstas Informacijos saugos priemones;

7.2.13.2. Informacijos saugos auditas turi būti atliekamas periodiškai, ne rečiau kaip kartą per 2 metus arba įvykus esminiams organizaciniams, sisteminiams ar kitokiems pokyčiams. Informacijos saugos audito priemonės negali stabdyti Įmonių veiklos.

8. ATSAKOMYBĖ

8.2. Jeigu Darbuotojas pažeidžia šios Politikos nuostatas, toks pažeidimas gali būti laikomas šiurkščiu darbo pareigų pažeidimu, už kurį gali būti taikoma Lietuvos Respublikos darbo kodekse įtvirtintos pasekmės, tarp jų, bet tuo neapsiribojant, darbo sutarties nutraukimas darbdavio iniciatyva dėl darbuotojo kaltės.
8.3. Grupės Įmonių ikisutartiniuose santykiuose ir sutartyse, tarp jų ir darbo sutartyse, turi būti užtikrinamas konfidencialumo įsipareigojimo laikymasis, raštu įtvirtinant šalių pareigą laikyti paslaptyje viena kitai perduodamą ar kitokiu būdu sužinotą informaciją tiek ikisutartinių santykių ar sutartinių santykių metu, tiek jiems pasibaigus ir susitariant dėl netesybų ir nuostolių atlyginimo konfidencialumo įsipareigojimo pažeidimo atveju.
8.4. Sudarant sandorius su Trečiosiomis šalimis, turi būti įtraukiami Trečiosios šalies įsipareigojimai laikytis šios Politikos nuostatų, taip pat nustatyti konkretūs su šia Politika suderinti pagal sudaromo sandorio pobūdį reikalingi Informacijos saugos reikalavimai ir atsakomybė už šios Politikos nuostatų nesilaikymą, tarp jų Grupės Įmonės teisė vienašališkai nutraukti sandorį, reikalauti netesybų ir nuostolių atlyginimo.

9. BAIGIAMOSIOS NUOSTATOS

9.2. Visi esami ir naujai priimami Darbuotojai, Kolegialių organų nariai, Paslaugų teikėjai bei kitos Trečiosios šalys, vykdančios sutartinius įsipareigojimus, privalo susipažinti su Politika ir įsipareigoti laikytis jos reikalavimų. Darbuotojų susipažinimas su Politika turi būti vykdomas priemonėmis, užtikrinančiomis susipažinimo įrodomumą.
9.3. Taikant šią Politiką turi būti vadovaujamasi ne tik šioje Politikoje nurodytais, bet ir kitais Grupės teisės aktais, susijusiais ir (ar) detalizuojančiais ir (ar) papildančiais šią Politiką.
9.4. Politika turi būti peržiūrima ne rečiau kaip kartą per metus ir, esant poreikiui, atnaujinama.
9.5. Ši Politika skelbiama Grupės centralizuotoje dokumentų valdymo sistemoje.

10. SUSIJĘ TEISĖS AKTAI

10.2. Grupės rizikos valdymo politika;
10.3. Grupės veiklos tęstinumo užtikrinimo politika;
10.4. Grupės asmens duomenų apsaugos politika;
10.5. Grupės informacijos konfidencialumo užtikrinimo standartas.