Patvirtinta:
Vičiūnų įmonių grupės
Valdybos pirmininkas Š.Matijošaitis
Įsakymo Nr. A25-083, 2025-09-24

VIČIŪNŲ ĮMONIŲ GRUPĖS INFORMACIJOS SAUGOS POLITIKA

TURINYS

POLITIKOS KEITIMO CHRONOLOGIJA			
Keitimo nr.	Data	Keitimo pobūdis	Keitimą atliko
1.			

1. TIKSLAS

1.1. Informacijos saugos politikos (toliau – **Politika**) **tikslas** yra nustatyti pagrindinius informacijos saugos tikslus, valdymo principus ir atsakomybes, užtikrinti nuolatinį informacijos saugos valdymo sistemos tinkamumą ir adekvatumą „Vičiūnų“ įmonių grupės strateginiams tikslams, veiksmingumą ir palaikymą pagal veiklos, teisinius, įstatyminius, reguliavimo ir sutartinius reikalavimus.

1.2. „Vičiūnų“ įmonių grupė (toliau – **Grupė**) įsipareigoja užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą, nepriklausomai nuo formos, kuria ji yra saugoma – popierine ar elektronine, taip pat apsaugoti nuo neteisėto jos naudojimo ir atskleidimo.

2. TAIKYMO SRITIS

2.1. Politika taikoma visoms Grupės Įmonėms ir privaloma visiems Grupės Įmonių Darbuotojams bei pagal kitus sutartinius pagrindus atliekantiems darbo funkcijas asmenims – praktikantams, ar laikinai darbo funkcijas atliekantiems asmenims, paslaugų teikėjams bei kitiems tretiesiems asmenims, kurie naudojasi ar yra tiesiogiai susiję su Grupės informaciniais ištekliais, nepriklausomai nuo jų buvimo vietos.

2.2. Kiekviena Bendrovė savo darbuotojus supažindina su Politika ir ją papildančiais dokumentais Bendrovėje nustatyta tvarka.

2.3. Tretieji asmenys užtikrina atitiktį šios politikos reikalavimams pasirašytų sutarčių ar kitokia teisine forma prisiimtų įsipareigojimų pagrindu, sudarytų atsižvelgiant į šios Politikos ir ją įgyvendinančių teisės aktų nuostatas. Tretieji asmenys, kurių darbuotojai atlieka veiklas Bendrovėje, įsipareigoja užtikrinti tų darbuotojų supažindinimą su šia Politika bei informuoti apie pareigą jos laikytis.

2.4. Politika ir kiti susiję dokumentai, turi būti peržiūrimi ne rečiau kaip kartą per metus ir iškilus poreikiui, inicijuojami reikiami pakeitimai.

2.5. Politika yra skelbiama viešai ir yra prieinama Grupės vidiniame tinklapyje bei internetinėje svetainėje.

3. BENDROSIOS NUOSTATOS

3.1. Ši Politika parengta remiantis ES ir nacionaliniais teisės aktais, aprašant jų taikymą ir įgyvendinimą Grupės veikloje, susijusioje su informacijos saugumu bei asmens duomenų apsauga

3.2. Pagrindiniai informacijos saugą Grupėje reglamentuojantys teisės aktai:

3.2.1. Lietuvos Respublikos kibernetinio saugumo įstatymas, kuriame į Lietuvos teisę perkelti ES TIS2 (Tinklų ir informacijos saugos direktyvos) reikalavimai;

3.2.2. Bendrasis Duomenų Apsaugos Reglamentas (**BDAR**);

3.2.3. 2018 m. birželio 30 d. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. XIII-1426 (toliau – **ADTAĮ**);

3.3. Politika paruošta remiantis šiais dokumentais, standartais, o taip pat gerosiomis informacinių technologijų (toliau – IT) praktikomis:

3.3.1. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir tvarkytojams (VDAI gairės);

3.3.2. LST EN ISO 27001:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ (ISO 27001 standartas);

3.3.3. LST EN ISO 27002:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (ISO 27002 standartas);

4. SĄVOKŲ APIBRĖŽIMAI

4.1. **Asmens duomenys** – bet kokia informacija apie asmenį (duomenų subjektą), pavyzdžiui, darbuotojo, kliento vardas, pavardė, asmens kodas, sistemoje suteiktas kodas, atvaizdas, paso kopija, batų ar darbo drabužių dydis, IP adresas, interneto naršymo istorija, planšetės geo-lokaciniai duomenys ir t.t., kuri leistų tiesiogiai arba netiesiogiai nustatyti fizinio asmens tapatybę.

4.2. **Bendrovė -** reiškia bet kurią Grupei priklausančią įmonę (nepriklausomai nuo teisinės formos), įskaitant ir Valdymo įmonę.

4.3. **Darbuotojas** – Bet kuris Grupės darbuotojas, dirbantis pagal darbo sutartį ar kitą sutartinį pagrindą (pvz. praktikos sutartis, funkcijų vykdymas pagal sutartį vykdymas remiantis individualios veiklos sutartimi ar verslo liudijimu) paskirtoje darbo vietoje bei vykdantis darbdavio paskirtas funkcijas.

4.4. **Dirbtinis Intelektas (DI)– t**ai kompiuterinės programos ar algoritmai, gebantys analizuoti duomenis, priimti sprendimus ir atlikti užduotis, paprastai reikalaujančias žmogaus intelekto. Jos pasitelkia mašininį mokymąsi, neuroninius tinklus ar kitus pažangius metodus, kad galėtų prisitaikyti, optimizuotis ir veikti dinamiškoje aplinkoje.

4.5. **Informacija –** apima visą nepriklausomai nuo formos (elektroninė ar popierinė ar kt.) bei jos saugojimo vietos esančią informaciją ir duomenis, susijusius su Bendrove ir / ar Grupės veikla, įskaitant, bet neapsiribojant, dokumentus, nuotraukas / vaizdo medžiagą, dokumentų projektus, kopijas, laiškus, memorandumus, schemas, planus, korespondenciją, Grupės klientų ir tiekėjų kontaktinius duomenis, programinės įrangos kodą, slaptažodžius, ar bet kokią kitą Bendrovės veikloje svarbią informaciją.

4.6. **Informaciniai ištekliai** – Grupės Informacija, tvarkomos Informacinės sistemos, informacinių technologijų funkcionavimui reikalingos paslaugos, darbuotojų žinios.

4.7. **Informacijos sauga** – Informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimas.

4.8. **Informacinė sistema** – apima programinę įrangą ir informacijos sistemas, esančias Grupės serveriuose, darbuotojų naudojamuose įrenginiuose (kompiuteriai, telefonai, planšetės, išorinės

laikmenos, tinklo infrastruktūra, sisteminė (operacinės sistemos, archyvavimo programinė įranga, kt.), duomenys, kiti kompiuteriniai komponentai ar sistemos, kurie priklauso Grupei ar yra naudojami Grupės reikmėms. Tokioms informacinėms sistemoms priklauso visos vidinės ir išorinės paslaugos, kaip debesijos kompiuterijos (cloud computing) būdu teikiamos paslaugos, Interneto prieiga, elektroninis paštas, komunikacijos priemonės.

4.9. **Techninė įranga** – apima visą ir bet kokią Grupei priklausančią techninę įrangą (angl. *hardware*), įskaitant, bet neapsiribojant, kompiuterius (įskaitant personalinius, nešiojamus ir planšetinius kompiuterius), išorinius įrenginius (USB diskus ar atmintines, skaitytuvus, monitorius, klaviatūras, peles, kolonėles, ausines, mikrofonus ir pan.), periferinę įrangą (spausdintuvus, kopijavimo, skenavimo, fakso aparatus ir pan.), kompiuterių tinklo įrangą, projektorius, fotoaparatus, nepertraukiamo elektros maitinimo šaltinius, stacionarių telefonų aparatus ir pan.

4.10. **Lankytojas** – gamintojo, partnerio atstovai, aptarnavimo specialistai, darbuotojo svečias ir bet kuris asmuo, kuris atvyksta į Grupei priklausančias patalpas ir nėra Grupės darbuotojas.

4.11. **Informacijos saugos incidentas** – įvykis, kuris sukelia pavojų Grupės informacijos ir/ar bet kurios jos informacinės sistemos vientisumui, konfidencialumui ar prieinamumui ir pažeidžia teisės aktus, šią Politiką, Grupės saugumo procedūras bei Grupės įmonių veiklą reglamentuojančias tvarkas arba kelia tokio pažeidimo grėsmę..

4.12. **Konfidencialumas** – tai leistinų prieigos ir atskleidimo apribojimų išsaugojimas, kuris taikomas užtikrinant asmens duomenų privatumą ir komercinių paslapčių apsaugą.

4.13. **Pasiekiamumas** – Informacijos ir informacinių sistemų savybė būti prieinama, kai reikia ir kur reikia.

4.14. **Vientisumas** – Informacijos savybė, reiškianti, kad informacija visą jos gyvavimo ciklą buvo tiksli ir nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

4.15. **Kibernetinės saugos vadovas –** Grupės generalinio direktoriaus paskirtas darbuotojas, administruojantis informacijos saugos klausimus Grupėje.

4.16. **Duomenų apsaugos pareigūnas (DAP)** – Grupės generalinio direktoriaus paskirtas asmuo, kuris konsultuoja asmens duomenų apsaugos reikalavimų klausimais Grupėje.

4.17. **Naudotojas** – Darbuotojas, rangovas ar kitas trečias asmuo, kuriam teisėtai suteikta prieiga prie Grupės Informacinių išteklių.

4.18. **Grupė –** reiškia įmonių grupę, kurią sudaro Valdymo įmonė ir visos jos tiesiogiai ar netiesiogiai valdomos įmonės (įskaitant įmones, kurios Grupei nepriklauso tačiau turi tos įmonės akcijų).

4.19. **Valdymo įmonė** reiškia UAB „Vičiūnų grupė“, kuri šios Politikos prasme taip pat yra ir Bendrovė.

4.20. **VPN** – Virtualus Privatus Tinklas (Virtual Private Network), technologinės priemonės skirtos saugiam prisijungimui prie Bendrovės informacinių išteklių

5. ATSAKOMYBĖS

5.1. Už šios Politikos valdymą, priežiūrą ir įgyvendinimą atsakingi asmenys:

5.1.1. Grupės Valdyba;

5.1.2. Kibernetinės saugos vadovas;
5.1.3. Duomenų apsaugos pareigūnas (DAP);
5.1.4. Infrastruktūros skyriaus vadovas;
5.1.5. Visi darbuotojai.

5.2. **Grupės valdybos** atsakomybė informacijos saugos srityje:
5.2.1. tvirtina šią Politiką bei nustato Informacijos saugos užtikrinimo tikslus ir principus Grupėje.
5.2.2. suteikia įgaliojimus bei paskiria atsakingus asmenis už Informacijos ir asmens duomenų saugą;
5.2.3. tvirtina informacijos saugumą reglamentuojančius dokumentus;
5.2.4. nustato priimtiną informacijos saugos lygį Grupėje;
5.2.5. užtikrina reikiamus išteklius ir resursus šios Politikos įgyvendinimui.

5.3. **Kibernetinės saugos vadovo** atsakomybė:
5.3.1. įgyvendina ir kontroliuoja Politikos įgyvendinimą (vykdo kontrolės funkciją);
5.3.2. nagrinėja ir svarsto klausimus, susijusius su Informacinių išteklių sauga ir jų naudojimu;
5.3.3. nagrinėja, analizuoja ir kontroliuoja klausimus, susijusius su Informacijos saugos incidentais, bendradarbiauja su kompetentingomis institucijomis;
5.3.4. organizuoja kasmetinį ir neeilinį (esant poreikiui) Informacijos saugos rizikos vertinimą;
5.3.5. užtikrina, kad Grupėje vadovaujamasi informacijos saugą reglamentuojančiais teisės aktais;
5.3.6. organizuoja veiklos tęstinumo valdymo plano bandymus;
5.3.7. teikia siūlymus ir organizuoja darbuotojų mokymus informacijos saugos klausimais;
5.3.8. teikia Sistemų administratoriui rekomendacijas susijusias su Politikos įgyvendinimu, kurios turi būti suderintos su IT plėtros vadovu arba jo paskirtu asmeniu ;
5.3.9. bendradarbiauja su DAP asmens domenų apsaugos klausimais;

5.4. Už asmens duomenų apsaugos reikalavimų įgyvendinimo priežiūrą atsakingas **Duomenų apsaugos pareigūnas** (toliau – DAP), kurio detalios funkcijos išdėstytos „Asmens duomenų politika“ dokumente.

5.5. **Infrastruktūros skyriaus vadovas:**
5.5.1. pagal aiškiai įmonės nustatytas taisykles suteikia, keičia ir panaikina Naudotojams prieigos teises prie Grupės Informacinių sistemų, apmoko bei konsultuoja Naudotojus;
5.5.2. vykdo kompiuterinių darbo vietų, veikimo koordinavimą, nustato pažeidžiamas vietas;
5.5.3. užtikrina kompiuterių tinklo tinkamą veikimą;
5.5.4. užtikrina tarnybinių stočių tinkamą veikimą;
5.5.5. užtikrina duomenų bazių ir duomenų bazių archyvo, atsarginio kopijavimo įrangos veikimą;
5.5.6. atsako už duomenų atsarginių kopijų darymą, saugojimą ir duomenų iš atsarginių kopijų atkūrimą bei saugą;
5.5.7. vykdo Informacijos saugos vadovo nurodymus ir pavedimus, susijusius su saugos užtikrinimu (vykdo priemonių įgyvendinimo funkciją).

5.6. **Visi Darbuotojai, dirbantys su informacinėmis sistemomis ir informacija** privalo:

5.6.1. laikytis Informacijos saugos reikalavimų, nustatytų šioje Politikoje;
5.6.2. laikytis Asmens duomenų apsaugos reikalavimų;
5.6.3. laikytis konfidencialumo įsipareigojimų, kurie galioja visą darbo laiką Grupėje ir nutraukus ar pasibaigus darbo ar sutartiniams santykiams;
5.6.4. nedelsiant pranešti apie silpnąsias vietas, pastebėtus galimus ar įvykusius informacijos saugos įvykius ir incidentus pagal nustatytą informacijos saugos incidentų valdymo tvarką;
5.6.5. naudoti Informacinius išteklius, kaip numatyta vidaus tvarkoje;
5.6.6. saugoti savo slaptažodį ar kitus prisijungimo ar autentifikacijos duomenis, neatskleisti jų ar neperduoti autentifikacijai naudojamų priemonių (pvz. atrakinto išmaniojo telefono) kitiems asmenims;
5.6.7. laikytis slaptažodžiams ir kitiems autentifikacijos būdams, pvz. PIN kodams nustatytų reikalavimų.

5.7. Pasekmės nesilaikant Politikos:
5.7.1. Darbuotojai, kurie nesilaiko ar pažeidžia šią Politiką ir susijusius dokumentus, gali būti baudžiami už darbo pareigų pažeidimą, atskirais atvejais Bendrovė taip pat gali kreiptis į teisėsaugos institucijas.
5.7.2. Galimos pasekmės Trečiosioms šalims (ar jų darbuotojams), kurios nesilaiko ar pažeidžia šią politiką – galimi sutarčių nutraukimai, patirtų nuostolių išieškojimas bei kitos pasekmės numatytos už sutarčių nesilaikymą.
5.7.3. Ignoravimas, geri ketinimai ir/ar priimti neteisingi sprendimai negali būti laikomi pateisinama priežastimi nesilaikyti šios Politikos.

6. KOMPETENCIJOS

6.1. Už Politikos priežiūrą ir vykdymo organizavimą paskirti atsakingi asmenys turi gerai išmanyti informacijos saugos, asmens duomenų apsaugos ir kibernetinio saugumo užtikrinimo principus, savo veikloje vadovautis Lietuvos Respublikos įstatymais ir teisės aktais reglamentuojančiais Informacijos saugą, kibernetinį saugumą ir asmens duomenų apsaugą. Išmanyti rizikos vertinimo metodikas ir principus.

7. INFORMACIJOS SAUGOS RIZIKOS VERTINIMAS

7.1. Grupės informacijos sauga užtikrinama įgyvendinat rizikų vertinimu pagrįstas saugos priemones. Informacijos saugos rizikų vertinimas yra sudėtinė ir neatsiejama Bendrovių rizikų valdymo proceso dalis.
7.2. Už informacijos saugos rizikų valdymo proceso inicijavimą, priežiūrą ir nuolatinį tobulinimą, surinktos informacijos apibendrinimą, komunikavimą, rizikos valdymo plano parengimą ir įgyvendinimo kontrolę atsakingas Kibernetinės saugos vadovas.
7.3. Už poveikio veiklai ir grėsmių vertinimą atsakingi Bendrovės informacinių išteklių valdytojai (savininkai), IT personalas, Darbuotojai pagal kompetencijų sritis.

8. INFORMACIJOS SAUGOS PRIEMONĖS IR ĮSIPAREIGOJIMAI

8.1. Remiantis rizikos valdymu, Grupėje numatytos šios organizacinės ir techninės Informacijos saugos priemonės, užtikrinančios Informacijos saugą (bet neapsiribojant):

8.2. **Atsakomybė už turtą:**

8.2.1. Informacija ir jos tvarkymui naudojama Techninė įranga turi nustatytą materialiai atsakingą asmenį. Šis asmuo yra atsakingas už šios Techninės įrangos ir Informacijos konfidencialumą, vientisumą ir prieinamumą.

8.2.2. Informacija ir Techninė įranga yra paskiriama sudarius darbo ar kitą sutartį ir grąžinama, kai baigiasi darbo ar kita sutartis.

8.2.3. Grupėje sudarytas „**Informacinių išteklių registras**“, kuriame identifikuotos Informacinės sistemos ir techninės priemonės Informacijai, tame tarpe ir Asmens duomenims apdoroti (kompiuterinės darbo vietos, tarnybinės stotys, tinklo įranga, informacinės sistemos), paskirti informacinių išteklių savininkai, kurie atsakingi už tinkamą informacinio ištekliaus priežiūrą ir informacijos saugos reikalavimų nustatymą priskirtam informaciniam ištekliui. Registras reguliariai, kas 3 mėnesius, peržiūrimas ir atnaujinamas, už registro tvarkymą atsakingas Kibernetinės saugos vadovas.

8.2.4. Visi Grupės Informaciniai ištekliai turi būti apskaitomi ir dokumentuojami, nurodant išteklių (ar grupės) valdytoją, susijusią techninę informaciją, fizinę vietą.

8.3. **Informacinių išteklių naudojimo sauga:**

8.3.1. Visi Informaciniai ištekliai gali būti naudojami tik Grupės veiklos funkcijoms atlikti.

8.3.2. Kiekvienas Darbuotojas turi būti pasirašytinai supažindintas su jam taikomais informacinių išteklių naudojimo reikalavimais.

8.3.3. Prieš nutraukiant darbo santykius visi suteikti Informaciniai ištekliai (informacijos saugojimo, perdavimo, apdorojimo priemonės, dokumentacija, nešiojamos duomenų laikmenos) turi būti grąžinti Bendrovei.

8.4. **Švaraus stalo ir švaraus ekrano politika:**

8.4.1. Darbuotojai privalo laikytis „švaraus stalo ir švaraus ekrano“ politikos, t. y. pasitraukus iš darbo vietos įjungti slaptažodžiu apsaugotą ekrano užsklandą, baigus darbą - išjungti visas programas ir kompiuterį, ant stalo esančius dokumentus ir duomenų laikmenas sudėti į stalčius ar spintas, o, jeigu informacija yra konfidenciali arba sudaranti komercinę (gamybos) paslaptį – į rakinamus stalčius ir spintas arba seifus, nebereikalingus svarbius arba konfidencialius dokumentus ir duomenų laikmenas neatkuriamai sunaikinti.

8.5. **Nuotolinio darbo sauga:**

8.5.1. Bendrovė privalo užtikrinti saugų nuotolinį darbą ir mobilių įrenginių naudojimą.

8.5.2. Nuotolinei prieigai galima naudoti tik saugius ir Bendrovės suteiktus prisijungimo metodus ir priemones. Bendrovės Darbuotojams leidžiama jungtis prie Bendrovės informacinių išteklių tik iš Bendrovės darbui išduotų kompiuterių. Savavališka nuotolinė prieiga prie Bendrovės informacinių išteklių griežtai draudžiama.

8.5.3. Nuotolinis prisijungimas prie Bendrovės Informacinių išteklių (pvz.: prieiga prie debesijos paslaugų, VPN prie vidinio kompiuterinio tinklo resursų ir t.t.) per viešuosius tinklus (internetą), realizuojama privalomai naudojant dviejų (ar daugiau) faktorių

autentifikaciją, todėl, siekiant papildomai patvirtinti besijungiančiojo tapatybę, naudojamas su Bendrovės informaciniais ištekliais susietas mobiliojo ryšio telefonas.

8.5.4. Bendrovė turi teisę pasitelkdama programinius įrankius valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą.

8.5.5. Nuotoliu dirbantys Naudotojai atsako už tai, kad tretieji asmenys prisijungimo sesijos metu neprieitų prie Bendrovės informacinių išteklių, t. y. paliekant savo darbo vietą privaloma atsijungti nuo vidinio tinklo, užrakinti kompiuterį.

8.5.6. Darbuotojas privalo laikytis šios Politikos ir kitų Bendrovėje galiojančių teisės aktų nepriklausomai nuo to, ar jis dirba Bendrovės patalpose ar nuotoliu.

8.6. **Informacijos klasifikavimas:**

8.6.1. Bendrovės informacija skirstoma pagal poreikį saugai ir teisinius reikalavimus. Konfidencialios informacijos ir komercinę (gamybos) paslaptį sudarančios informacijos sąrašas ir informacijos valdymo reikalavimai nustatyti Vičiūnų įmonių grupės „**Konfidencialumo sutartis**“.

8.7. **Prieigos teisių valdymas:**

8.7.1. Valdant prieigą prie Bendrovės informacinių išteklių, turi būti užtikrintas principo „būtina darbui“ ir „mažiausių teisių prieigos“ įgyvendinimas, t. y. toks prieigos prie Bendrovės informacinių išteklių reikalavimas, kuris reiškia, kad prieiga gali būti suteikta tik patvirtintiems asmenims ir tokia apimtimi, kuri yra būtina vykdant konkrečias darbo ir kitas su Bendrove susijusias funkcijas.

8.7.2. Prieigos valdymas turi būti dokumentuotas. Naudotojų ir administratorių prieigos teisės informacinėse sistemose turi būti peržiūrimos ne rečiau kaip kartą per metus arba esant reikšmingiems pokyčiams Bendrovėje ar incidentams.

8.8. **Kriptografijos priemonių naudojimas:**

8.8.1. Saugaus elektroninės informacijos teikimo ir (arba) gavimo užtikrinimui duomenys teikiami šifruotais duomenų perdavimo kanalais, naudojant specialius protokolus.

8.9. **Atsarginių kopijų kūrimas ir valdymas:**

8.9.1. Visų Bendrovės veiklai svarbių duomenų ir programinės įrangos atsarginės kopijos turi būti atliekamos periodiškai. Atkūrimas iš atsarginių kopijų turi būti išbandomas ne rečiau kaip kartą per metus su bandymo rezultatų ataskaita supažindinant Kibernetinės saugos vadovą. Atsarginės kopijos turi būti saugomos saugiu atstumu nuo pagrindinių sistemų – rezerviniame duomenų centre, debesijos paslaugų sistemose. Atsarginių kopijų dažnumas, apimtis, metodai ir saugojimo terminas turi atitikti sistemos RTO (Recovery Time Objective – priimtinas sistemos atkūrimo laikas ir RPO (Recovery Point Objective – priimtinas prarastų duomenų kiekis) reikalavimus.

8.10. **Pažeidžiamumų valdymas:**

8.10.1. Visos darbo vietos, tarnybinės stotys, tinklo įrenginiai ir kt. turi įdiegtas saugumo pataisas tam, kad Informacinės sistemos būtų apsaugotos nuo pažeidžiamumų.

8.11. **Informacijos perdavimo sauga:**

8.11.1. Grupėje yra taikomos duomenų saugumo technologijos. Perduodant konfidencialią ar vidinio naudojimo Informaciją bet kokiu kanalu (e-mail, sftp, https, kt.), naudojami stipraus šifravimo algoritmai.

8.11.2. Perduodant popierinius dokumentus, duomenys pieš perduodant turi būti inventorizuoti, tinkamai užregistruoti.

8.11.3. Naudotojai, prieš talpindami informaciją į pasirinktą išorinę laikmeną, turi atsižvelgti į Informacijos klasifikavimo reikalavimus.

8.12. **Keitimų valdymas:**

8.12.1. Keitimų valdymo tikslas sinchronizuoti ir kontroliuoti visus Informacinėse sistemose, kuriose apdorojama Grupės Informacija ir Asmens duomenys, atliekamus pakeitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas pakeitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą.

8.12.2. Poreikis keitimams gali iškilti dėl įvairių priežasčių, įskaitant, bet neatsiribojant, žemiau išvardintiems:

- patvirtinti naudotojų prašymai;
- tiekėjų paslaugų pasikeitimai;
- techninės ar programinės įrangos atnaujinimai;
- naujos techninės ar programinės įrangos diegimai;
- infrastruktūros pasikeitimai.

8.12.3. Bendrovė užtikrina, kad visi Informacinių sistemų pakeitimai būtų stebimi ir registruojami paskirto asmens (Sistemų administratorius).

8.13. Grupėje yra naudojamos apsaugos nuo žalingo programinės įrangos kodo priemonės.

8.14. **Įvykių registravimas ir stebėsena:**

8.14.1. Grupė turi teisę ir pareigą atlikti visų Informacinių sistemų, įskaitant visus įrenginius, kurie jungiasi prie Informacinių sistemų ar naudojasi sistemomis, stebėseną bei stebėti (registruoti) visus duomenis, kaupiamus Grupės Informacinėse sistemose ir / arba siunčiamus Grupės tinklais. Tokio registravimo pavyzdys yra žurnalinių įrašų (angl. logs) kaupimas registruojant pvz. darbuotojo prisijungimą prie konkrečios informacinės sistemos. Ši stebėsena nereiškia Darbuotojų stebėsenos ar jų veiksmų kontrolės darbo pareigų atlikimo kokybės vertinimo tikslu.

8.15. Grupėje yra naudojamos Tinklo valdymo priemonės.

8.16. **Duomenų saugojimas, naikinimas, šalinimas:**

8.16.1. Duomenys, kurie nėra reikalingi, yra saugiai sunaikinami. Elektroniniai duomenys ištrinami neatkuriamu būdu ar sunaikinama laikmena, popieriniai – sunaikinami dokumentų naikikliu.

8.16.2. Pašalinant (baigtas tarnavimo laikas) ar laikinai perduodant (pvz., remontui) iš darbo aplinkos duomenų laikmenas, duomenys turi būti užšifruoti tinkamo saugumo šifravimo algoritmais arba sunaikinti.

8.16.3. Grupėje vengiama ir tik kraštutiniu atveju gali būti naudojamos išorinės laikmenos, kaip duomenų laikmenos, CD / DVD ir pan.

8.16.4. Kompiuterinių laikmenų ir jose esančios informacijos sunaikinimą atlieka darbuotojai, atsakingi už Techninės įrangos priežiūrą.

8.17. **Dirbtinio intelekto sistemų naudojimo sauga:**

8.17.1. Atsižvelgiant į dažną DI sistemų naudojimą šiuolaikinėje darbinėje aplinkoje, taip pat būtina atsižvelgti į šių sistemų keliamas rizikas.

8.17.2. Netinkamas DI sistemų naudojimas gali atskleisti konfidencialią Bendrovės informaciją ar kitą intelektinę nuosavybę, kai yra naudojamos netinkamai (pvz. viešosios ar asmeninės DI paslaugos kurios naudojamos darbiniams uždaviniams atlikti), kai Bendrovės informacija yra pateikiama tokioms sistemoms, o po to Darbuotojui to nežinant ir nekontroliuojant panaudojama minėtų sistemų apmokymui ir kitais būdais.

8.17.3. Bet koks DI sistemų naudojimas Bendrovės ar konfidencialiai verslo partnerių ar trečiųjų šalių informacijai apdoroti neįvertinus jų keliamų rizikų yra draudžiamas. Įvertinant galimas rizikas turi dalyvauti specialistai turintys pakankamą žinių lygį DI srityje.

8.17.4. Bendrovė gali suteikti Darbuotojams galimybę naudoti izoliuotas DI sistemas (kurios nesikeičia informacija su viešąja aplinka, t.y. Internetu) ir kurių taikymas Bendrovėje yra leistas vadovybės.

8.17.5. Rezultatai, gauti DI sistemų naudojimo pagalba turi būti vertinami kritiškai ir papildomai patikrinti, atsižvelgiant į tai, jog DI sistemos gali pateikti klaidingą informaciją.

9. FIZINĖ IR APLINKOS VEIKSNIŲ SAUGA

9.1. Informacinių išteklių saugumas Bendrovėje turi būti užtikrinimas kaip Bendrovės fizinės saugumo sistemos dalis.

10. SANTYKIAI SU TIEKĖJAIS BEI KITOMIS TREČIOSIOMIS ŠALIMIS

10.1. Tiekėjams prieiga prie Grupės informacijos ir (ar) Informacinių išteklių gali būti suteikiama tik tokios apimties, kiek tai būtina sutarčiai įgyvendinti ir nedelsiant panaikinama, pasibaigus sutartiniams santykiams.

10.2. Sutartyse su tiekėjais, kuriems turi būti suteikta prieiga prie Grupės Informacijos ir (ar) Informacinių išteklių, turi būti įtraukti „Minimalūs informacijos ir kibernetinės saugos reikalavimai tiekėjams“ (priedas Nr.1.)

11. ŽMOGIŠKŲJŲ IŠTEKLIŲ SAUGA

11.1. Prieš suteikiant prieigą prie Bendrovių informacinių išteklių asmuo turi būti pasirašytinai susipažinęs su informacijos saugos pareigomis ir atsakomybe, nurodytais: darbo sutartyje, Asmens duomenų tvarkymo politikoje, Informacijos saugos politikoje, darbo tvarkos taisyklėse ir kituose vidaus dokumentuose.

11.2. Sutartyse su Trečiaisiais asmenimis turi būti numatytos sutarties šalių informacijos saugos pareigos ir atsakomybės.

11.3. Bendrovės darbuotojų ir, jei aktualu, Trečiųjų asmenų, informacinių technologijų ir telekomunikacijų naudojimo ir informacijos saugos žinios turi būti pakankamos darbo

funkcijoms atlikti. Kiekvienas Darbuotojas turi būti apmokytas kaip atpažinti informacijos saugos grėsmes/incidentus; taikyti saugos priemones ir metodus; pranešti apie informacijos saugos incidentus.

11.4. Darbuotojų saugos žinių lygis turi būti vertinamas ir, jei reikalinga, atliekami papildomi mokymai.

12. INFORMACIJOS SAUGOS INCIDENTŲ VALDYMAS

12.1. Apie visus įvykusius ar įtariamus informacijos saugumo incidentus ir įvykus (pvz.: Įrangos ar informacijos praradimas, kompiuteriniai virusai, šio Tvarkos aprašo pažeidimai ir pan.) ar saugumo spragas, silpnas saugumo vietas turi būti nedelsiant informuojamas **Kibernetinės saugos vadovas** ir IT departamentas: **el. paštu soc@vici.eu, it-help@vici.eu** arba telefonu +370 67059912.

12.2. Visi Darbuotojai, Tretieji asmenys ir kiti susiję asmenys turi pareigą pranešti apie saugos incidentus, aiškiai nurodant, kokiomis priemonėmis ir kas yra informuojamas apie incidentus.

12.3. Informacijos saugos incidentai (ir saugos įvykiai) turi būti sistemingai ir nuosekliai valdomi, užtikrinant tinkamą ir savalaikį reagavimą į juos bei incidentų poveikio ateityje mažinimą, kaip tai numatyta Informacijos saugos incidentų valdymo procese.

12.4. Informacija apie įvykusius saugos incidentus, „išmoktas pamokas“, siūlymai incidentų valdymo tobulinimui stebimi rodiklių pagalba ir aptariami pasitarimų metu. Taip pat ši informacija naudojama rizikų identifikavimui bei stebėsenai vykdyti.

12.5. Asmens duomenų saugos pažeidimų valdymą reglamentuoja Bendrovės Asmens duomenų saugumo pažeidimų reagavimo tvarka. Į asmens duomenų saugos incidentų valdymą įtraukiamas Duomenų apsaugos pareigūnas.

13. VEIKLOS TĘSTINUMO VALDYMAS

13.1. Bendrovės veiklos tęstinumo valdymas informacijos saugos incidentų atveju turi būti integruotas į Bendrovės veiklos tęstinumo sistemą ir valdomas taikant vieningus reikalavimus visai organizacijai.

13.2. Kiekvienai bendrovės veiklai esminei informacinei sistemai turi būti parengtas informacinės sistemos tęstinumo/atkūrimo planas.

13.3. Veiklos tęstinumo plano veiksmingumas tikrinamas kiekvienais metais, imituojant kritines situacijas, kurių metu paskirti atsakingi asmenys atlieka kritinės situacijos veiksmus. Pastebėti trūkumai ir pažeidžiamumai analizuojami ir nustatomos gerinimo priemonės.

14. INFORMACIJOS SAUGOS AUDITAS

14.1. Bendrovės informacijos saugos auditas ir atitikties Lietuvos Respublikos teisės aktų reikalavimams vertinimas, atliekamas periodiškai, tačiau ne rečiau kaip: kartą per metus atliekamas atitikties Lietuvos Respublikos teisės aktų reikalavimams vertinimas. Vertinimą atlieka Bendrovės Kibernetinės saugos vadovas.

14.2. Bendrovės atitikties asmens duomenų apsaugos reikalavimams vertinimas atliekamas ne rečiau kaip kartą per metus. Vertinimą atlieka Bendrovės Duomenų apsaugos pareigūnas.

14.3. kartą per 3 metus atliekamas išorinis Informacijos saugos auditas. Auditą atlieka Grupės audito padalinys arba įmonės, turinčios kvalifikuotus šios srities specialistus su ne mažesne nei 3 metų patirtimi informacijos saugos audito srityje.
14.4. Auditų fiksuotos rekomendacijos ir neatitiktys turi būti įvertintos ir sudaromas priemonių planas informacijos saugos gerinimui.

PRIEDAI

Nr.1. Minimalūs informacijos ir kibernetinės saugos reikalavimai tiekėjams