PATVIRTINTA
Valstybės įmonės Valstybinių miškų urėdijos
generalinio direktoriaus
2022 m. gegužės 12 d. įsakymu Nr. ĮS(E)-70

VALSTYBĖS ĮMONĖS VALSTYBINIŲ MIŠKŲ URĖDIJOS INFORMACIJOS SAUGOS POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės įmonės Valstybinių miškų urėdijos informacijos saugos politika (toliau – Politika) yra skirta pateikti vieningus ir veiksmingus informacijos saugos užtikrinimo kryptis ir principus, suvaldyti informacijos saugos grėsmių riziką bei užtikrinti efektyvų informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Informacija yra viena vertingiausių valstybės įmonės Valstybinių miškų urėdijos (toliau – Įmonė) turto dalių, todėl jos praradimas, neteisėtas pakeitimas ar atskleidimas, sugadinimas ir informacijos apdorojimo nutraukimas gali sukelti Įmonės veiklos sutrikimų, padaryti žalos kitiems fiziniams ir juridiniams asmenims. Neskiriant pakankamo dėmesio ir resursų informacijos saugos rizikos valdymui, didėja pavojus prarasti konkurencingumą laisvoje rinkoje, patirti finansinę ir reputacinę žalą, nepasiekti Įmonei iškeltų tikslų.

3. Pagrindiniai informacijos saugos užtikrinimo tikslai Įmonėje:

3.1. užtikrinti saugią ir patikimą informacinę ir kibernetinę aplinką;

3.2. užtikrinti informacijos saugumą: informacijos konfidencialumą, vientisumą ir prieinamumą;

3.3. užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;

3.4. užtikrinti ir valdyti atitiktį teisės aktų, reglamentuojančių informacijos saugą ir kibernetinį saugumą bei asmens duomenų apsaugą, reikalavimams.

4. Politika taikoma visai Įmonėje naudojamai informacijai (nepriklausomai nuo jos formato, laikmenos ir saugojimo būdo), visiems procesams, visiems Įmonės darbuotojams bei valdybos ir Audito komiteto nariams, taip pat kitų Įmonėje sudarytų komitetų nariams, fiziniams ir juridiniams asmenims, kuriems teisės aktų ar sutartinių santykių pagrindu yra suteikta prieiga prie Įmonės informacijos ar informacijos apdorojimo priemonių, taip pat jų ir Įmonės teikiamoms paslaugoms.

5. Politika ir ją įgyvendinantys vidaus teisės aktai rengiami atsižvelgiant į tarptautinius informacijos saugos standartus (LST ISO / IEC 27001, LST ISO / IEC 27002 ir kt.) ir pasaulines gerosios informacijos saugos praktikas, taip pat atspindi esamus technologinius pokyčius ir informacijos saugos grėsmių tendencijas bei užtikrina Europos Sąjungos ir Lietuvos Respublikos teisės aktų, reglamentuojančių informacijos saugą ir kibernetinį saugumą, ar sutartinių įsipareigojimų laikymąsi.

II SKYRIUS
INFORMACIJOS SAUGOS UŽTIKRINIMO KRYPTYS IR PRINCIPAI

6. Informacijos saugos užtikrinimo principai:

6.1.	Principas „būtina žinoti“	Įmonės konfidenciali, komercinę paslaptį sudaranti informacija ir (ar) prieigos teisės prie jos Įmonės darbuotojams, Įmonės valdybos nariams ir tretiesiems asmenims gali būti suteikta tik tiek, kiek būtina vykdant konkrečias darbo ir kitas su Įmone susijusias funkcijas, įsipareigojimus pagal Įmonės sutartis ar Lietuvos Respublikos teisės aktuose numatytas pareigas ir tik

		pasirašius nustatytos formos Įsipareigojimą neatskleisti konfidencialios informacijos.
6.2.	Atitikties reikalavimams principas	Įmonė, užtikrindama informacijos apsaugą, atsižvelgia į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), Lietuvos Respublikos kibernetinio saugumo įstatyme, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir kituose teisės aktuose informacijos apsaugai keliamus reikalavimus, Lietuvos standartus LST ISO/IEC 27001 ir LST ISO/IEC 27002 ir kitus Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus bei į tarptautinę gerąją praktiką.
6.3.	Informacijos apsauga turi remtis rizikos valdymo procesu	Nustatoma, kokia informacija Įmonėje valdoma; įvertinami informacijos praradimo ir nesankcionuoto atskleidimo tikimybė ir poveikis; planuojamos ir įgyvendinamos organizacinės ir techninės priemonės, kurios padėtų sumažinti riziką iki priimtino lygio. Politika nuolatos peržiūrima ir atnaujinama.
6.4.	Veiklos tęstinumo principas	Įmonėje parengiami veiklos tęstinumo planai, kuriuose numatomas esminių funkcijų ir jų vykdymui būtinos informacijos atkūrimas. Tęstinumo planai turi būti išbandomi, komunikuojami, taip pat vykdomi darbuotojų apmokymai.

7. Informacijos saugos užtikrinimo kryptys:

7.1. **Mokymai ir švietimas**. Įmonėje turi būti vystoma informacijos saugos kultūra, kad Įmonės darbuotojai tinkamai suvoktų informacijos ir jos saugos svarbą, galimą neigiamą poveikį Įmonės veiklai, Įmonės keliamų tikslų įgyvendinimui. Turi būti nuolatos didinamas visų Įmonės darbuotojų atsparumas informacijos saugos grėsmėms periodiškai organizuojant mokymus, tikrinant darbuotojų žinias, vykdant nuolatinę komunikaciją apie Įmonei aktualias informacijos saugos grėsmes ir priemones, leidžiančias išvengti informacijos saugos ar kibernetinio saugumo incidentų.

7.2. **Rizikos valdymas**. Įmonės svarbiausių veiklos procesų, informacinių technologijų ir informacijos saugos grėsmių rizika turi būti vertinama periodiškai, taip pat ir atsiradus poreikiui (kuriant naujas ar keičiant esamas informacines technologijas, informacines sistemas, procesus). Identifikuota rizika turi būti mažinama iki toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstas, kainos ir efektyvumo atžvilgiu subalansuotas bei informacijos saugą reglamentuojančius teisės aktus ir tarptautinius standartus atitinkančias informacijos saugos priemones.

7.3. **Informacinis turtas**. Įmonės didžiausią vertę turintis informacinis turtas (Įmonės konfidenciali informacija, komercinės paslaptys) turi būti identifikuotas bei paskirti už jį atsakingi informacinio turto savininkai. Informacinio turto savininkai turi reguliariai (ne rečiau kaip kartą per metus) peržiūrėti prie informacinio turto suteiktas prieigos teises ir imtis reikiamų veiksmų, esant neatitikimams.

7.4. **Atitiktis**. Turi būti įgyvendinami Įmonės sutartiniai įsipareigojimai su trečiosiomis šalimis, Įmonės vidaus bei išorės teisės aktų informacijos saugos reikalavimai, taikant rizikos vertinimu pagrįstas informacijos saugos priemones.

7.5. **Santykiai su trečiosiomis šalimis**. Informacijos, kuria keičiamasi su trečiųjų šalių partneriais, tiekėjais, saugumas turi būti užtikrintas visu sutarčių galiojimo metu, į sutartis įtraukiant informacijos saugos nuostatas, įpareigojančias informacijos gavėjus užtikrinti ne mažesnį informacijos saugos lygį, nei kad taikomas Įmonėje.

7.6. **Incidentų ir pažeidžiamumų valdymas**. Informacijos saugos ar kibernetinio saugumo incidentai (ir saugumo įvykiai) bei pažeidžiamumai turi būti sistemingai ir nuosekliai valdomi, registruojami, užtikrinant reikiamą reagavimą, suvaldymą ir mokymąsi iš incidentų, siekiant išvengti incidentų pasikartojimo ar pažeidžiamumų išnaudojimo.

7.7. **Aiški savininkystė**. Įmonės informacinių sistemų ir jų procesų savininkai (turintys sprendimų teisę ir valdantys reikalingus išteklius) yra atsakingi už tinkamą informacijos saugos ir kibernetinių grėsmių rizikos valdymą.

III SKYRIUS
DALYVIAI IR ATSAKOMYBĖS

8. Įmonės valdyba nustato informacijos saugos užtikrinimo kryptis, siekius ir principus Įmonėje.

9. Informacijos saugos atitiktį užtikrinantys darbuotojai su Technologijų vadovo pritarimu formuoja Įmonės informacijos saugos strategiją, organizuoja Įmonės informacijos saugos rizikos identifikavimą, teikia pagalbą Įmonei suvaldant rizikas.

10. Įmonės vadovybė informacijos saugos rizikos klausimus laiko neatsiejama Įmonės veiklos procesų dalimi, skiria tinkamą dėmesį ir išteklius informacijos saugos rizikos valdymui.

11. Įmonės darbuotojai užtikrina informacijos saugumą kasdienėje veikloje priimdami sprendimus, atlikdami veiksmus, suderintus su nuostatomis reglamentuojančiomis informacijos saugą.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

12. Su Politika turi būti supažindinti visi priimami į darbą ir esami Įmonės darbuotojai.

13. Politika tvirtinama, keičiama ar pripažįstama netekusia galios Įmonės generalinio direktoriaus įsakymu. Politikos nuostatas įgyvendinančius vidaus teisės aktus taip pat tvirtina Įmonės generalinis direktorius įsakymu.

14. Politikos nuostatos peržiūrimos kas 2 (dvejus) metus arba anksčiau, jeigu atsiranda tokia būtinybė, o jos peržiūrą inicijuoja Prevencijos skyrius.

15. Politika skelbiama Įmonės intranete ir viešai Įmonės interneto svetainėje.

16. Pažeidus šios politikos ar kitų teisės aktų, susijusių su informacijos sauga, nuostatas, darbuotojams taikoma atsakomybė teisės aktų nustatyta tvarka.