Kvalifikuotas elektroninis parašas
UGNIUS JANKAUSKAS
2025-05-19 11:23:39 EEST
Paskirtis: Parašas

UAB „VERSLO ŽINIOS“
INFORMACIJOS SAUGOS POLITIKA

I. ĮVADAS

1. Informacija yra vienas vertingiausių UAB „Verslo žinios“ (toliau – Bendrovė) išteklių, todėl jos elektroninės, rašytinės ir žodinės informacijos apsauga yra esminis siekis, norint užtikrinti Bendrovės patikimumą, finansinį stabilumą, veiklos tęstinumą, konkurencinį pranašumą ir suinteresuotų šalių reikalavimų vykdymą.

2. Atsižvelgdama į informacijos svarbą ir vertę bei atsakomybę, Bendrovė imasi priemonių informacijos saugumui užtikrinti, kuriomis siekiama išvengti veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo, autentiškumo bei prieinamumo pažeidimų.

3. Šia politika Bendrovė įsipareigoja apsaugoti jos ir klientų informaciją nuo tyčinio, neatsargaus ir neleistino pakeitimo, sunaikinimo, atskleidimo ar panaudojimo ne pagal paskirtį ar teisinę praktiką.

4. Šia politika Bendrovė įsipareigoja įgyvendinti, prižiūrėti ir nuolatos tobulinti Bendrovės informacijos saugumo valdymo sistemą (toliau – INFOSEC) ir jos efektyvumą vadovaujantis patirtimi, įgyta ją įgyvendinant ir vykdant jos stebėseną, skirti pakankamai materialinių ir žmogiškųjų resursų, rūpintis darbuotojų švietimu informacinių rizikų srityje ir INFOSEC atitiktimi galiojantiems teisės aktams, suinteresuotų šalių lūkesčiams ir Bendrovės strategijai.

5. Šia politika Bendrovė įsipareigoja puoselėti „Just Culture“ kultūrą, kurioje Bendrovė įsipareigoja netraukti drausminėn atsakomybėn darbuotojų, kurie netyčiniais veiksmai ar neveikimu pažeidė INFOSEC ar sukėlė INFOSEC grėsmę ir apie tai pranešė, Informacijos saugos pareigūnui, Bendrovės vadovui ar savo tiesioginiams vadovams.

II. INFORMACIJOS SAUGUMO VALDYMO SISTEMA

6. Šią politiką įgyvendina INFOSEC - dokumentuotas procesų ir kontrolės priemonių derinys, įgyvendinamas siekiant apsaugoti informaciją nuo įvairių grėsmių ir užtikrinti jos konfidencialumą (apsauga nuo neteisėto ar atsitiktinio atskleidimo), vientisumą (apsauga nuo neteisėto ar atsitiktinio informacijos pakeitimo), autentiškumą (informacija yra patikima ir atitinka tikrovę, t.y. nepakeista, nesuklastota ir nesusijusi su sukčiavimu ar apsimetinėjimu) ir prieinamumą (informacija prieinama tada, kai ji reikalinga).

7. INFOSEC taikoma visose Bendrovės veiklos srityse, visuose padaliniuose, apima žodinę, rašytinę ir skaitmeninę Bendrovės informaciją, informacinę ir fizinę infrastruktūrą, aplinką, darbuotojus bei procesus, o taip pat santykius su trečiosiomis šalimis.

8. INFOSEC taikoma visiems Bendrovės tvarkomos ir saugomos informacijos gyvavimo ciklams: sukūrimui, tvarkymui, saugojimui ir sunaikinimui.

9. INFOSEC kryptys:

9.1. Sistemingas saugumo kultūros formavimas ugdant darbuotojų informacinio saugumo kompetencijas ir tinkamą elgesį;

9.2. Bendrovės ir klientų informacijos apsauga nuo vidinių ir išorinių, sąmoningų, atsitiktinių ar kitokių grėsmių bei informacijos saugumo rizikų mažinimas;

9.3. Tinkamų, geriausią praktiką atitinkančių saugumo priemonių įgyvendinimas nustatytoms rizikoms mažinti, atsižvelgiant į periodinius elektroninės informacijos saugumo rizikos vertinimus;

Verified by MarkSign.lt

9.4. INFOSEC incidentų ir pažeidžiamumų sistemingas ir nuoseklus valdymas, užtikrinant reikiamą reagavimą, suvaldymą ir mokymąsi iš incidentų, siekiant išvengti incidentų pasikartojimo ar pažeidžiamumų išnaudojimo.

9.5. Nuolatinis Informacijos saugumo valdymo sistemos tobulinimas pagal tarptautinių standartų reikalavimus ir rekomendacijas.

10. Už informacijos saugumą atsako visi Bendrovės darbuotojai ir trečiosios šalys, kurioms perduodama Bendrovės ar jos klientų informacija ar kurios teikia paslaugas, susijusias su šia informacija.

11. Informacijos saugumą Bendrovėje organizuoja paskirtas informacijos saugumo vadovas.

12. Bendrovė reikalauja, kad informacijos, kuria keičiamasi su trečiosiomis šalimis, saugumas būtų užtikrintas visų sutarčių galiojimo metu, tiek savarankiškai pačių tiekėjų, tiek ir sutartiniais įsipareigojimais, įpareigojančias Informacijos gavėjus užtikrinti ne mažesnį jiems patikėtos informacijos saugos lygį, nei taikomas Bendrovėje.

III. BAIGIAMOSIOS NUOSTATOS

13. INFOSEC valdymo sistemą sudaro ši politika, INFOSEC proceso aprašas su priedais.

14. Politika peržiūrima ne rečiau nei kartą per metus ir atnaujinama esant poreikiui, atsižvelgiant į INFOSEC metinės vertinamosios analizės rezultatus, Bendrovės strategiją, suinteresuotųjų šalių lūkesčius.

_____

Verified by MarkSign.lt