ASMENS DUOMENŲ SAUGUMAS
ATMINTINĖ DARBUOTOJAMS

Asmens duomenų saugumo pažeidimas (toliau – ADSP) sudaro sąlygas piktavaliams perimti asmens duomenis, kurie gali būti panaudojami kibernetiniams incidentams ir nusikaltimams vykdyti.

Siekdama padėti sumažinti riziką patirti ADSP, Valstybinė duomenų apsaugos inspekcija pateikia patarimų, kaip sustiprinti duomenų apsaugą.

Siūlomos įgyvendinti organizacinės priemonės:

Supraskite, kokius duomenis turite, ir juos klasifikuokite. Negali apsaugoti informacijos, jei nežinai, kur ji saugoma ar kaip naudojama, kur laikomos atsarginės kopijos ir t. t. Įsitikinkite, kad žinote, kokie duomenys jūsų organizacijoje yra kritiškai svarbūs ar jautrūs, juos būtina suklasifikuoti pagal svarbos ar kritiškumo lygį.

Užtikrinkite fizinę dokumentų ir įrenginių su duomenimis saugą – laikykite asmens duomenis saugiai, kad niekas neturėtų prieigos be jūsų leidimo.

Nuolat laikykitės „švaraus stalo“ ir „švaraus spausdintuvo“ taisyklių, jokie dokumentai su asmens duomenimis neturi likti be Jūsų priežiūros.

Būtinai nurodykite atgalinį adresą, kai siunčiate siuntas ar pašto vokus su dokumentais, kad per klaidą juos gavęs kitas asmuo galėtų grąžinti siuntą jos neatidaręs.

****

Siūlomos įgyvendinti techninės priemonės:

Slaptažodžiai

Kiekvienas kompiuteris privalo būti apsaugotas slaptažodžiu.

Slaptažodžių kompleksiškumo reikalavimai:

- Unikalus, sudarytas iš ne mažiau kaip 8 simbolių;
- Naudojama kombinacija su didžiosiomis, mažosiomis raidėmis ir bent vienas skaitmuo bei papildomas simbolis ?, !, &, £, % ir kt.;
- Slaptažodyje nenaudojami darbuotojo asmeninio pobūdžio informacija: vardas, pavardė, gimimo data bei kiti, lengvai nuspėjami slaptažodžiai, tokie kaip „slaptažodis“, „1234“ ir pan.;

Slaptažodžiais privalo būti apsaugoti ne tik kompiuteriai, bet darbui naudojamos programos (sistemos) ir kitos elektroninio ryšio priemonės, naudojamos darbui, t. y. mobilieji telefonai, planšetiniai kompiuteriai.

Būtina užtikrinti, kad **slaptažodžiai nebūtų išsaugomi** sistemose, programose, viešai matomose ar kitaip kitiems asmenims laisvai prieinamose vietose.

Slaptažodžių keitimo periodiškumas

Slaptažodžiai privalo būti periodiškai keičiami. Periodiškumą nustato Įmonė atskiru vidiniu dokumentu.

Vadovaujantis gerąja praktika, visi slaptažodžiai privalo būti keičiami **ne rečiau kaip vieną kartą per 6 (šešis) kalendorinius mėnesius**, jei kitokių terminų nenustato Įmonės vidiniai dokumentai ar duomenų apsaugą reglamentuojantys teisės aktai.

****

Duomenų saugojimas ir prieigų kontrolė

Visi dokumentai su asmens duomenimis, saugomi Įmonės naudojamuose saugiuose (patikimuose) **serveriuose / debesyse**.

Draudžiama saugoti asmens duomenis kompiuteryje ir išorinėse laikmenose (USB raktuose, išoriniuose kietuosiuose diskuose ir pan.), kurių prieiga nėra apsaugota slaptažodžiu, persiųsti asmens duomenis į asmeninį elektroninį paštą.

Jei keli darbuotojai, darbo funkcijų vykdymo tikslais, naudoja bendrą kompiuterį, **kiekvienam darbuotojui turi būti sukurta atskira vartotojo paskyra**, apsaugota tik tą paskyrą naudojančiam darbuotojui žinomu slaptažodžiu.

Specialių kategorijų asmens duomenys (pvz., informacija apie sveikatą, biometriniai duomenys ir kt.) privalo būti saugomi tik **saugiuose serveriuose/debesyse**, turi būti užtikrintas specialių kategorijų duomenų **šifravimas**, serveriai periodiškai tikrinami dėl saugumo ir apsaugomi kompleksiškais slaptažodžiais.

****

Apsauga nuo trečiųjų šalių prieigos prie asmens duomenų

Darbuotojai privalo užtikrinti, kad:

- Tretiesiems asmenims (ne darbuotojams) nebus suteikta prieiga naudotis kompiuteriu, telefonu ir kitomis elektroninio ryšio priemonėmis, skirtomis darbui, kurios yra Įmonės nuosavybė;
- Nesilankys nesaugiose internetinėse svetainėse;
- Nesisiųs nelegalios programinės įrangos;
- Nespaus ant neaiškių nuorodų į svetaines bei neatidarinės „spam“ laiškų;
- Nedarys Įmonei priklausančiame kompiuteryje, telefone ar kitoje elektroninio ryšio priemonėje esančių duomenų atsarginių kopijų;
- Visas iš interneto, nešiojamųjų ir kitų duomenų laikmenų siunčiamas programas ir informaciją patikrins naudojant teisėtai įdiegtą kompiuterių virusus atpažįstančią (antivirusinę) programą;
- Įmonei priklausančiuose kompiuteriuose ar kitose kompiuterizuotose darbo vietose naudos ekrano užsklandą su slaptažodžio apsauga; draudžiama palikti kompiuterį ar kitą kompiuterizuotą darbo vietą neišjungtą arba neaktyvavus slaptažodžiu apsaugotos ekrano užsklandos; Nepaliks kompiuterio, telefono be priežiūros (transporto priemonėje, viešose vietose ir pan.).

****

„Wi-Fi“ apsauga

Draudžiama suteikti prieigą prie Įmonės vidinio *„Wi-Fi“* tinklo tretiesiems asmenims (ne darbuotojams). Prireikus suteikti prieigą, privalo būti sukurtas atskiras, slaptažodžiu apsaugotas, prieigos kanalas.

****