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.

➢ 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.

****

Slaptažodžiai

Kiekvienas kompiuteris privalo būti apsaugotas slaptažodžiu.

Slaptažodžių kompleksiškumo reikalavimai:

- Unikalus, sudarytas iš ne mažiau kaip 10 simbolių;
- Slaptažodį sudaro bent trijų tipų simboliai (didžiosios, mažosios raidės, skaičiai ar specialieji simboliai);
- Slaptažodis keičiamas ne rečiau kaip vieną kartą per 6 mėnesius (180 kalendorinių dienų);
- Slaptažodyje neturi būti naudojama darbuotojo asmeninio pobūdžio informacija (pvz.: gimimo data, šeimos narių vardai ir pan.);
- Naudotojas pirmą kartą gavęs administratoriaus suteiktą naudotojo vardą ir slaptažodį, turi prisijungti prie Ligoninės informacinės sistemos ir nedelsdamas pakeisti slaptažodį ir jį įsiminti;
- Naudotojai privalo saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;
- Naudotojas įtaręs, kad tretieji asmenys sužinojo jo slaptažodį, privalo nedelsdamas jį pakeisti.

Slaptažodžiais privalo būti apsaugoti ne tik kompiuteriai, bet ir 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 prieinamuose vietose.

****

Duomenų saugojimas ir prieigų kontrolė

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 Ligoninės nuosavybė;

❖ Nesilankys nesaugiose internetinėse svetainėse;

❖ Nesisiųs nelegalios programinės įrangos;

❖ Nespaus ant neaiškių nuorodų į svetaines bei neatidarinės „spam“ laiškų;

❖ Nedarys Ligoninei 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;

❖ Ligoninei priklausančiuose kompiuteriuose ar kitose kompiuterizuotose darbo vietose naudos ekrano užsklandą su slaptažodžio apsauga;

❖ Draudžiama palikti kompiuterį ar kitą kompiuterizuotą darbo vietą be priežiūros, neaktyvavus slaptažodžiu apsaugotos ekrano užsklandos;

❖ Nepaliks darbo kompiuterio, telefono be priežiūros (transporto priemonėje,viešose vietose ir pan.).

****