PATVIRTINTA
Vilniaus Antakalnio progimnazijos
2025 m. liepos 15 d.
direktoriaus įsakymu Nr. V-18

VILNIAUS ANTAKALNIO PROGIMNAZIJOS IT INFRASTRUKTŪROS SAUGUMO UŽTIKRINIMO TAISYKLĖS

1. BENDROSIOS NUOSTATOS

1.1. Vilniaus miesto savivaldybės biudžetinė įstaiga, Vilniaus Antakalnio progimnazija, įmonės kodas 302818006, buveinės ir korespondencijos adresas: Antakalnio g. 33, LT-10312 Vilnius, tel. Nr.: +370 659 00612, el. paštas: rastine@antakalnio.lt *(toliau – Įstaiga arba Duomenų valdytoja)*, vadovaujantis Bendruoju Duomenų Apsaugos Reglamentu (ES) 2016/679 *(toliau - BDAR)*, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu *(toliau - ADTAĮ)* ir kitais Europos Sąjungos ir Lietuvos Respublikos teisės aktais, reguliuojančiais fizinių asmenų *(toliau – Duomenų subjektas)* asmens duomenų apsaugą ir tvarkymą, siekiant tinkamai įgyvendinti BDAR reikalavimus, šiose Įstaigos IT infrastruktūros saugumo užtikrinimo taisyklėse *(toliau – Taisyklės)* nustato Duomenų subjektų asmens duomenų ir Įstaigos IT infrastruktūros saugumo tvarką.

1.2. Taisyklės taikomos visiems Įstaigos darbuotojams, kurie naudojasi Įstaigos IT infrastruktūra, ir apima įrenginių saugumą, prieigą prie sistemų, failų saugojimą, tinklo saugumą, ryšių ir fizinį saugumą.

2. ĮSTAIGOS ĮRENGINIŲ SAUGA

2.1. Įstaigos darbuotojai turi imtis saugos priemonių dirbdami su Įstaigos (Duomenų valdytojo) darbo įrenginiais *(pvz., kompiuteriais, planšetiniais kompiuteriais ir išmaniaisiais telefonais),* nes įrenginiai gali būti pavogti, paveikti kenkėjiškų programų ir naudojami asmenų, neturinčių tam teisės.

2.2. Įstaigos kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai visada turi būti stebimi arba laikomi saugioje vietoje. Kai jie nenaudojami, šie prietaisai turi būti užrakinti su PIN arba slaptažodžio apsauga, arba išjungti.

2.3. Siekiant užkirsti kelią neteisėtai prieigai prie Įstaigos įrenginyje saugomos informacijos, visi Įstaigos kompiuteriai, planšetiniai kompiuteriai ir išmanieji telefonai turi turėti įdiegtus šifravimo sprendimus.

2.4. Įstaigos darbuotojams į savo kompiuterius negalima atsisiųsti Įstaigos programinės įrangos. Jei Įstaigos darbuotojui į kompiuterį reikia atsisiųsti išorinę programinę įrangą, jis turėtų gauti Įstaigos direktoriaus leidimą ir patvirtinimą.

2.5. Įstaigos kompiuteriuose iš anksto turi būti įdiegtos apsaugos nuo kenkėjiškų programų. Jei antivirusinė programa informuoja apie grėsmę ir kompiuteris veikia neįprastai arba Įstaigos darbuotojui kyla abejonių dėl naudojamos įrangos apsaugos nuo kenkėjiškų programų, jis privalo nedelsdamas (bet ne ilgiau kaip per 24 val.) apie tai pranešti Įstaigos direktoriui žodžiu, raštu ar elektroninėmis priemonėmis, nutraukti darbą kompiuteriu ir išjungti jį iš tinklo.

2.6. Jei Įstaigos darbuotojas turi prieigą prie Įstaigos IT sistemos, kurios jam nebereikia vykdant savo pareigas, jis privalo apie tai nedelsdama pranešti Įstaigos direktoriui žodžiu, raštu ar elektroninėmis priemonėmis.

3. ĮSTAIGOS INFORMACIJOS SAUGA

3.1. Kai Įstaigos darbuotojui suteikiamas laikinas slaptažodis prisijungti prie Įstaigos IT sistemos, Įstaigos darbuotojas privalo nedelsiant pakeisti laikiną slaptažodį po pirmojo prisijungimo prie Įstaigos IT sistemos ir jo negalima užsirašyti arba dalintis su kitais Įstaigos IT sistemos vartotojais.

3.2. Įstaigos darbuotojas negali suteikti prieigos teisių prie Įstaigos IT sistemos kitiems vartotojams.

3.3. Įstaigos darbuotojas yra atsakingas už saugų savo darbo failų *(pvz., MS Word / Excel / PowerPoint rinkmenų)* tvarkymą ir turi būti labai atsargūs saugodami Duomenų subjektų asmens duomenis failuose.

3.4. Įstaigos darbuotojas privalo apriboti dalijimąsi failais, kuriuose yra Duomenų subjektų asmens duomenų, kad būtų užkirstas kelias pažeidimams ar netinkamam šių duomenų naudojimui, ir turi ištrinti Duomenų subjektų asmens duomenis, kurių jam nebereikia vykdant savo pareigas. Tai taikoma visiems failams, kuriuos sukūrė Įstaigos darbuotojas, įskaitant MS Word / Excel / PowerPoint failus.

3.5. Įstaigos darbuotojams draudžiama naudoti ir saugoti Įstaigos (Duomenų valdytojo) vardu tvarkomų Duomenų subjektų asmens duomenų ir informacijos ne Įstaigos įrenginiuose, nes kyla duomenų praradimo grėsmė.

4. ĮSTAIGOS TINKLO SAUGUMAS

4.1. Įstaigos mobilieji įrenginiai turi būti jungiami tik prie Įstaigos „Wi-Fi“ tinklo, skirto mobiliesiems įrenginiams. Kiti kompiuteriai ar mobilieji įrenginiai turi būti jungiami prie Įstaigos svečių „Wi-Fi“ tinklo.

4.2. Įstaigos darbuotojams draudžiama jungtis prie Įstaigos klientų tinklo be išankstinio Įstaigos kliento sutikimo, nebent Įstaigos klientas yra nurodęs viešus prisijungimo duomenis.

4.3. Įstaigos darbuotojai turėtų būti atsargūs, kai naudojasi viešaisiais „Wi-Fi“ tinklais. Duomenų srautas per viešuosius tinklus gali būti stebimas. Prieš naudodamiesi viešaisiais „Wi-Fi“ tinklais, Įstaigos darbuotojai turėtų įsitikinti, kad „Wi-Fi“ tinklas yra apsaugotas ir gaunamas iš teisėto paslaugų teikėjo.

4.4. Jei yra priežasčių abejoti viešojo „Wi-Fi“ tinklo saugumu, Įstaigos darbuotojas turėtų vietoj jo naudoti mobiliojo ryšio tinklą savo darbinėms funkcijoms atlikti.

4.5. Naršymas asmeniniais tikslais Įstaigos darbuotojams leidžiamas tik svetainėse, kurių turinys suderinamas su Įstaigos darbuotojo darbo funkcijomis.

4.6. Įstaigos darbuotojams internetiniai žaidimai ar azartiniai lošimai draudžiami, o failų bendrinimas ar srautinis medijos transliavimas internetu turėtų apsiriboti su darbu susijusiu turiniu.

4.7. Visi Įstaigos darbuotojai turėtų žinoti, kad Įstaigos administracija analizuoja interneto srautą, siekiant nustatyti atakas prieš Įstaigą, o taip pat gaunama informacija apie netinkamą interneto naudojimą.

5. ĮSTAIGOS DARBUOTOJŲ KOMUNIKACIJA

5.1. El. paštas yra svarbi skaitmeninė Įstaigos darbuotojų komunikacijos priemonė. Tai ir pagrindinis informacijos saugumo pažeidžiamumo šaltinis, nes jis suteikia atakuotojams galimybę nukreipti į Įstaigos IT sistemą kenkėjiškas programas, užsiimti sukčiavimu ir kitomis grėsmėmis patiriant mažas sąnaudas ir su maža baudžiamojo persekiojimo rizika. Dažnas tapatybės sukčiavimo *(„phishing“)* atvejis yra, kai „sukčius“ tiesiogiai kreipiasi į Įstaigos darbuotoją. El. laiškas atrodo tarsi būtų siųstas iš patikimo šaltinio, dažnai naudojant netikrą tapatybę kito Įstaigos darbuotojo, partnerio ar pardavėjo. El. laišku bandoma paveikti Įstaigos darbuotoją, kad jis atliktų laiške nurodytus veiksmus *(pvz., pervestų pinigus, įvestų prisijungimo / slaptažodžio duomenis ar kitą slaptą informaciją)*, paspaustų nuorodą ar atidarytų priedą, kuris parsiunčia kenkėjišką programinę įrangą *(„malware“)* į Įstaigos darbuotojo kompiuterį ar mobilųjį telefoną. Laiškas, jo priedas ar nuoroda gali atrodyti nekaltai – *pavyzdžiui*, bus užmaskuotas kaip kliento ar kolegos laiškas, tiekėjo pasiūlymas, sąskaita faktūra arba kaip debesijos paskyros *(„OneDrive“),* pranešimas. Dėl šios priežasties Įstaigos darbuotojai turi būti labai budrūs tvarkydami el. laiškus ar kitokio pobūdžio pranešimus, net jei jie atrodo gauti iš patikimo šaltinio.

5.2. Įstaigos darbuotojai turi neatidaryti nuorodų arba priedų savo prietaisuose, jei jie abejoja elektroninio laiško ar kitokio kontakto su juo teisėtumu ir privalo nedelsdami (bet ne ilgiau kaip per 24 val.) apie tai pranešti Įstaigos direktoriui ir Įstaigos IT specialistui žodžiu, raštu ar elektroninėmis priemonėmis, nutraukti darbą kompiuteriu ir išjungti jį iš tinklo.

5.3. Jei Įstaigos darbuotojas nėra tikras dėl elektroninio laiško teisėtumo arba jei netyčia sureagavo į galimą mėginimą sukčiauti, atidaręs įtartiną nuorodą ar priedą, jis privalo nedelsdamas (bet ne ilgiau kaip per 24 val.) pranešti apie šį incidentą Įstaigos direktoriui ir Įstaigos IT specialistui žodžiu, raštu ar elektroninėmis priemonėmis, nutraukti darbą kompiuteriu ir išjungti jį iš tinklo.

5.4. Įstaigos darbuotojo el. paštas neturėtų būti naudojamas svarbios Įstaigos informacijos archyviniam saugojimui. Įstaigos informacija turėtų būti saugoma arba ja dalinamasi saugiomis sistemomis ar failų bendrinimo sprendimais, o ne el. paštu.

5.5. Įstaigos darbuotojai turėtų būti labai atsargūs, dalydamiesi Įstaigos informacija socialinėje žiniasklaidoje. Tinkamai naudojamos socialinės žiniasklaidos priemonės suteikia Įstaigos darbuotojams galimybę įgyti ir perduoti žinias ir kurti santykius bet socialinės žiniasklaidos priemonės gali labai pakenkti Įstaigos ir jos darbuotojams, jei jos naudojamos netinkamai, arba jei dalijamasi konfidencialia informacija.

5.6. Bet kokius Duomenų subjektų asmens duomenis (įskaitant vardus, nuotraukas ir kt.) galima bendrinti tik su Įstaigos veiklą susijusiuose socialinės žiniasklaidos pranešimuose, jeigu Duomenų subjektas, kurio duomenys bus bendrinami, sutinka su jo asmens duomenų naudojimu.

6. ĮSTAIGOS PATALPŲ SAUGUMAS

6.1. Visus Įstaigos lankytojus reikia pasitikti Įstaigos priimamajame, o po vizito palydėti lankytoją iki išėjimo iš Įstaigos teritorijos.

6.2. Įstaigos lankytojų negalima palikti vienų Įstaigos patalpose ir/ar teritorijoje.

6.3. Visa konfidenciali informacija privalo būti pašalinta nuo Įstaigos darbuotojų darbo stalų ir saugiai laikoma, kai ji nenaudojama.

6.4. Pasibaigus susitikimams su Įstaigos lankytojais visos rašomosios lentos turi būti nuvalytos.

_____