PATVIRTINTA
Raseinių r. Šiluvos gimnazijos
direktoriaus 2024 m. gruodžio 19 d.
įsakymu Nr. V1-172

RASEINIŲ R. ŠILUVOS GIMNAZIJOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I. TIKSLAS

Informacijos ir kibernetinio saugumo politika (toliau – Politika) apibrėžia Raseinių r. Šiluvos gimnazijos (toliau – Gimnazija) poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje bei yra skirta pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Gimnazijos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

II. TAIKYMO SRITIS

Ši Politika privaloma visiems Gimnazijos darbuotojams, tiekėjams bei rangovams ir taikoma kiekviename Gimnazijos veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, valdomi procesai.

III. NUORODOS

Kibernetinio saugumo įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą.

IV. SĄVOKOS IR SANTRUMPOS

Informacija – bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis.

Informacijos saugumas – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Kai tai tikslinga, papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip atsakingumas, apskaita, autentiškumas/patikimumas, nepaneigiamumas ir privatumas.

Informacinė aplinka – individai (naudotojai), organizacijos ir/arba sistemos, kurios renka, apdoroja arba platina informaciją. Taip pat, ir pati informacija.

Informacinė sistema – informacijos apdorojimo sistemos ir organizacijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui.

Informaciniai ištekliai – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, mokymų medžiaga; programinė įranga, jos kūrimo priemonės; aparatinė įranga (duomenų laikmenos, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų

funkcionavimui reikalingos paslaugos; išorės šalių teikiamos paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.

Išorės šalys – paslaugų teikėjai, partneriai, kiti asmenys, turintys ar galintys turėti prieigą prie Gimnazijos informacinių išteklių.

Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija.

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.

Konfidencialumas – užtikrinimas, kad bet kokia Įstaigos informacija yra pasiekiama tik įgaliotiems asmenims, kuriems yra būtina žinoti, ir jiems suteikta tokia prieiga. Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir mokinių asmeninė informacija.

Vientisumas – užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklastojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo.

Prieinamumas – užtikrinimas, kad visada yra prieiga prie tam tikros informacijos, duomenų bazės ar kitų elektroninių paslaugų.

V. POLITIKOS ĮGYVENDINIMO TIKSLAI

1. Užtikrinti saugią ir patikimą informacinę ir kibernetinę erdvę.
2. Užtikrinti informacijos saugumą: informacijos konfidencialumą, vientisumą ir prieinamumą.
3. Užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą.
4. Ieškoti naujų būdų ir priemonių, užtikrinančių saugumą, tačiau nemažinančių patogumo naudotojams.
5. Užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

VI. PRINCIPAI

Gimnazija, siekdama užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

1. Padidintas dėmesys informacijos ir kibernetinio saugumo kultūros vystymui ir palaikymui. Darbuotojai turi tinkamai suvokti informacijos ir jos saugumo svarbą, galimą neigiamą poveikį Gimnazijos veiklai. Didinamas visų Gimnazijos darbuotojų atsparumas kibernetinėms grėsmėms, vykdant komunikaciją apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų.
2. Atitiktis. Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Gimnazijos sutartiniams įsipareigojimams su trečiosiomis šalimis, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones.
3. Sistemingas ir nuoseklus incidentų ir pažeidžiamumų valdymas. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų, siekiant išvengti jų pasikartojimo ar pažeidžiamumų išnaudojimo.

VII. ĮSIPAREIGOJIMAI

Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Gimnazija įsipareigoja:

1. Laikytis visų kibernetinio ir informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse ir prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemos efektyvumą.

2. Skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei vystyti Gimnazijos darbuotojų informacijos saugumo kultūrą ir kibernetinę higieną (sąmoningumą).

3. Užtikrinti efektyvų informacijos saugumo valdymo sistemos aprūpinimą reikiamais ištekliais, sudaryti sąlygas Gimnazijos darbuotojams tobulinti žinias informacijos ir kibernetinio saugumo bei asmens duomenų saugumo srityse.

VIII. POLITIKOS PERŽIŪRA IR SKLAIDA

1. Politika tvirtinama, keičiama ar naikinama Gimnazijos direktoriaus įsakymu. Politiką rengia, reguliariai peržiūri ir atnaujina Gimnazijos informacinių komunikacinių technologijų (IKT) specialistas, paskirtas direktoriaus įsakymu.

2. Politika yra skelbiama Gimnazijos interneto svetainėje www.siluvosgimnazija.lt ir prieinama visoms suinteresuotoms šalims.

3. Šios Politikos nuostatos įgyvendinamos priimant Gimnazijos vidaus teisės aktus, derančius su strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais ir gerosiomis praktikomis.

_____

Raseinių r. Šiluvos gimnazijos
informacijos ir kibernetinio
saugumo politikos
priedas

RASEINIŲ R. ŠILUVOS GIMNAZIJOS KIBERNETINIO SAUGUMO RIZIKOS VEIKSNIAI IR MAŽINIMO PRIEMONĖS

Kibernetinio saugumo rizikos išvengti neįmanomą, todėl svarbu užtikrinti tinkamą jos maksimalų valdymą. Tam būtina įsivertinti pažeidžiamiausias Gimnazijos sritis, atlikti grėsmės poveikio analizę bei suplanuoti priemonių taikymą. Kibernetinio saugumo rizikos vertinimas leidžia nustatyti rizikos grėsmės bei jų lygį Gimnazijoje. Vadovaujantis rizikos mažinimo priemonėmis galima sumažinti kibernetinių atakų skaičių arba jų poveikį Gimnazijai. Už kibernetinio saugumo rizikos vertinimą ir priemonių plano joms mažinti parengimą atsakingas direktoriaus įsakymu paskirtas informacinių technologijų mokytoja.

KIBERNETINIO SAUGUMO RIZIKOS TIPAI GIMNAZIJOJE

8. **Grėsmės internete:** tai didžiausia ir populiariausia rizikos grupė. Tai įvairūs tiesioginiai ir netiesioginiai išpuoliai, įsilaužimai, atakos. Internetinių grėsmių pavyzdžiai yra virusai, įsilaužimai, šlamšto el. laiškai, apgaulingos SMS žinutės.

2. **Vidinės grėsmės:** tai grėsmės kylančios dėl darbuotojų kaltės. Ji gali būti tyčinė arba atsitiktinė. Tai slaptažodžių atskleidimas, slaptos informacijos aptarimas su kolegomis, sąmoningas neskelbtinos informacijos atskleidimas.

3. **Fizinės grėsmės:** tai materialaus Gimnazijos turto (kompiuterių, serverių, kitų įrenginių) pažeidimas arba vagystė. Fizinės grėsmės kyla dėl stichinių nelaimių, teroristinių išpuolių ar tyčinio fizinio turto sugadinimo arba vagystės.

RIZIKOS LYGIO NUSTATYMAS

Lygis	Tikimybės apibrėžimas	Pavyzdys
Aukštas	Grėsmės šaltinis yra labai motyvuotas ir pakankamai pajėgus, o kontrolės priemonės, kuriomis siekiama užkirsti kelią pažeidžiamumui, yra neveiksmingos	Neteisėtas kenkėjiškas informacijos atskleidimas, kenkimas ar sunaikinimas
Vidutinis	Grėsmės šaltinis yra motyvuotas arba pajėgus, tačiau kontrolės priemonės gali trukdyti sėkmingai pasinaudoti pažeidžiamumu	Netyčinės klaidos ir pažeidimai
Žemas	Grėsmės šaltiniui trūksta motyvacijos ar gebėjimų, o taikomos kontrolės priemonės gali užkirsti kelią pažeidžiamumui	IT sutrikimai dėl stichinių ar žmogaus sukeltų nelaimių

DAŽNIAUSIAI GALINČIOS PASITAIKYTI RIZIKOS IR JŲ LYGIS

Rizika	**Rizikos lygis**	**Rekomendacijos**
Darbuotojas paspaudė nuorodą į užkrėstą svetainę	Aukštas	Užvesti pelės žymeklį ant nuorodas ir patikrinti ar adresas yra tikras, ar nėra gramatinių klaidų, pavadinimas yra logiškas
Darbuotojas atskleidė savo prisijungimo slaptažodį	Aukštas	Jei yra galimybė naudoti dviejų žingsnių autentifikavimą, nelaikyti slaptažodžiu atviru tekstu
Darbuotojas įdiegė kenksmingą programinę įrangą	Aukštas	Darbuotojams draudžiama savarankiškai diegti programas
Virusas pateko per atminties laikmeną	Aukštas	Nesinaudoti nepatikimomis laikmenomis, nuolat jas tikrinti su antivirusine programa
Iš vadovo gautas laiškas su neįprasta užduotimi	Aukštas	Patikrinti el. pašto dėžutės adresą, radus neatitikimų informuoti IKT specialistą
Virusas užkrėtė kompiuteryje esančius duomenys	Aukštas	Periodiškai daryti atsargines duomenų kopijas, saugoti duomenis bent dviejuose fiziškai atskirtuose vietose
Interneto ryšio dingimas	Vidutinis	Informuoti IKT darbuotoją arba interneto tiekėją. Kol ryšis atkuriamas pasinaudoti mobiliojo telefono saitviete (hot-spot)
Mokyklos interneto svetainės nulaužimas	Vidutinis	Atlikti svetainės atnaujinimus, tikrinti SSL sertifikato galiojimą ir jį laiku pratęsti
Svarbios įrangos fizinis pažeidimas arba vagystė	Žemas	Įranga laikyti saugiame, rakiname kabinete su ribota pašalinių asmenų patekimo galimybe

KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS MOKYKLOS LYGMENIU

1. **Slaptažodžių politika.** Įsitikinti, kad Gimnazijoje yra laikomasi saugaus slaptažodžio kūrimo ir naudojimo principų.

2. **Kelių žingsnių autentifikavimas.** Jei yra galimybė, naudoti aukštesnio lygio apsaugos priemones, kad būtų saugiai naudojamasi savo svarbiausiomis paskyromis.

3. Antivirusinės programos. Apsaugoti Gimnazijos kompiuterius ir kitus įrenginius nuo kenkimo programų ir užkrėstų dokumentų.

4. Atsarginės duomenų kopijos. Apsaugoti Gimnazijos dokumentus nuo informacijos nutekėjimo, vagysčių ar kitų nelaimių.

5. Prieigos kontrolė. Atskirti ir žinoti kokie darbuotojai gali pasiekti svarbią informaciją.

6. Išmokyti darbuotojai. Sumažinti žmogaus klaidų rizika šviečiant darbuotojus kibernetinio saugumo klausimais.

7. Automatiniai atnaujinimai. Įsitikinti, kad Gimnazijos kompiuteriai turi įdiegtą naujausią programinę įrangą.

8. Darbo ir asmeninių įrenginių atskyrimas. Įsitikinti, kad darbuotojais saugiai naudojasi savo įrenginiais

9. Ugniasienės. Sukurti saugią neutralią zoną tarp interneto ir Gimnazijos.

10. Saugus bevielis tinklas. Tinkamai prižiūrėti maršrutizatorius, kad kenkėjai nepatektų į Gimnazijos tinklą.

KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS DARBUOTOJO LYGMENIU

1. Neprijungti nežinomų USB atmintinių prie Gimnazijos kompiuterių.
2. Nepalikti neužrakinto kompiuterio net trumpam palikę savo darbo vietą. Galima nustatyti automatinio užsirakinimo funkciją.
3. Saugoti ir teisingai tvarkyti prisijungimo duomenis.
4. Neklijuoti ant ekranų ir nepalikti prisijungimo duomenų kitiems matomose vietose.
5. Niekam neatskleisti savo prisijungimo duomenų.
6. Nespausti ant nuorodų el. laiškuose, ypač gautuose iš nežinomų siuntėjų.
7. Neatskleisti pašaliniams jautrios asmeninės ar Gimnazijos informacijos.
8. Baigus darbą, uždaryti programų langus, išjungti kompiuterį. Nepalikti ant stalo dokumentų ir duomenų laikmenų.

_____