ქ. გორი

10.04.2020წ.

გრძანება N 01-32

შპს მეცნიერებათა სკოლის ინფორმაციული ტექნოლოგიების მართვის პროცედურების დამტკიცების შესახებ

შპს მეცნიერებათა სკოლის წესდების საფუძველზე,

ვბრძანებ:

1. დამტკიცდეს შპს მეცნიერებათა სკოლის ინფორმაციული ტექნოლოგიების მართვის პროცედურები დანართის შესაბამისად.
2. ბრძანება ძალაში შედის ხელმოწერისთანავე;
3. ბრძანება შეიძლება გასაჩივრდეს კანონმდებლობით დადგენილი წესით გაცნობიდან ერთი თვის ვადაში გორის რაიონულ სასამართლოში (მის.: ქ. გორი, სერგო ჯორბენაძის N30).

შპს მეცნიერებათა სკოლის

დირექტორი

სოფიო სუხიშვილი

ინფორმაციული ტექნოლოგიების მართვის პროცედურები

მუხლი 1. შესავალი

შპს მეცნიერებათა სკოლია (შემდგომში - სკოლა) ინფორმაციული ტექნოლოგიების მართვის პროცედურები განსაზღვრავს სკოლის საინფორმაციო ტექნოლოგიების IT რისკების მართვის, პერსონალურ მონაცემთა დაცვის, საინფორმაციო ინფრასტრუქტურისა და IT პროცესების სისტემის ეფექტიანობის მართვის, მოსწავლეებისა და პერსონალისათვის მუდმივად ხელმისაწვდომი IT ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის და მომსახურების წესებს.

მუხლი 2. ტერმინთა განმარტება

ა) **კონფიდენციალურობა** – ინფორმაციის ხელმისაწვდომობა მხოლოდ მასზე წვდომის უფლების მქონე პირთათვის, ასევე მოსწავლეებისა და პერსონალისთვის;
ბ) **მთლიანობა** – უტყუარი ცოდნა იმისა, რომ ძირითადი მონაცემები და ინფორმაცია არის სწორი, არ არის შეცვლილი განზრახ ან გაუფრთხილებლობით და ასახავს ზუსტ ფაქტებს;
გ) **ხელმისაწვდომობა** – უტყუარი ცოდნა იმისა, რომ ინფორმაცია საჭირო დროს იქნება ხელმისაწვდომი ავტორიზებული მომხმარებლებისათვის;
დ) **კონტროლის მექანიზმი** – ოპერაციების განხორციელებაზე შეზღუდვებისა და წესების შესრულების უზრუნველსაყოფად შექმნილი ქმედებების და ტექნოლოგიების ერთობლიობა;
ე) **ძირითადი ინფორმაცია** – სკოლის ძირითადი ფუნქციების შესრულებისთვის აუცილებელი ინფორმაცია;
ვ) **მეორეხარისხოვანი ინფორმაცია** – ყველა ის ინფორმაცია, რომელიც არ არის ძირითადი;
ზ) **ინფორმაციული აქტივი** – ყველა სახის ინფორმაცია, ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, მოსწავლეებისა და პერსონალის შესახებ ინფორმაცია და მათი ცოდნა ინფორმაციის დამუშავების შესახებ;
თ) **კრიტიკული სისტემები** – ინფორმაციული სისტემები, რომლებიც ამუშავებს ძირითად ინფორმაციას;
ი) **მესამე მხარე** – ფიზიკური ან იურიდიული პირი, რომელიც არ არის სკოლის მოსწავლე და პერსონალი ან/და წარმოადგენს სხვა იურიდიულ პირს.
კ) **საარქივო მასალა** – ინფორმაცია, რომელიც მნიშვნელოვანია სკოლისთვის, მაგრამ მიმდინარე ოპერაციების დროს არ გამოიყენება;
ლ) **ავტორიზებული მომხმარებელი** – სუბიექტი, რომელსაც სკოლის ადმინისტრაციისაგან გააჩნია თანხმობა ისარგებლოს ინფორმაციით, ინფორმაციული სისტემებით, ინფორმაციული ტექნოლოგიებით და ახორციელებდეს მათ მართვას. ასევე მოსწავლეები და პერსონალი;
მ) **სასიცოცხლოდ მნიშვნელოვანი სისტემა** – სისტემა, რომელზეც არასანქცირებულმა წვდომამ შესაძლოა გამოიწვიოს სკოლის ფუნქციონირების მნიშვნელოვანი შეფერხება.

მუხლი 3. ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი მიმართულებები

ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი მიმართულებებია:
ა) ორგანიზაციული უსაფრთხოება;
ბ) ინფორმაციული აქტივების მართვა;
გ) მოსწავლეებისა და პერსონალის უსაფრთხოება;
დ) ფიზიკური უსაფრთხოება;

ე) ინფორმაციული უსაფრთხოების ინციდენტების იდენტიფიცირება;
ვ) კომუნიკაციებისა და ოპერაციების მართვა;
ზ) წვდომის კონტროლის მართვა;
თ) ინფორმაციული სისტემების დანერგვა და მხარდაჭერა;
ი) კანონმდებლობასთან თავსებადობა.

მუხლი 4. ინფორმაციული უსაფრთხოების თანამშრომელი

ინფორმაციული უსაფრთხოების თანამშრომელი არის საინფორმაციო მენეჯერი და მის მოვალეობაში შედის სკოლაში არსებული ინფორმაციული უსაფრთხოების საკითხების მონიტორინგი, ინფორმაციული აქტივების და მასზე წვდომის აღწერა, ინციდენტების შეგროვება და მათზე რეაგირების მონიტორინგი.

მუხლი 5. პერსონალის და მოსწავლეების უსაფრთხოება

1. სკოლა უზრუნველყოფს ადამიანური ფაქტორის რისკის შესამცირებლად (შეცდომა, თაღლითობა, სისტემებზე წვდომის ბოროტად გამოყენება და ა.შ.) კონტროლის მექანიზმების დანერგვას.
2. პერსონალის და მოსწავლეების უსაფრთხოების უზრუნველსაყოფად სკოლა იყენებს სწავლების, ტრენინგისა და ინსტრუქტაჟის მეთოდებს.
3. ინფორმაციული უსაფრთხოების შესახებ ტრენინგი ან ინსტრუქცია (ასეთის არსებობის შემთხვევაში) ხელმისაწვდომი უნდა იყოს სუბიექტებისთვის.
4. სკოლა უზრუნველყოფს სუბიექტებისა და მესამე პირებისთვის განკუთვნილი ინფორმაციის უსაფრთხოებასთან დაკავშირებული ვალდებულებების შესახებ ინფორმაციის მიწოდებას და გაცნობას.

მუხლი 6. ფიზიკური უსაფრთხოება

1. სკოლა ახორციელებს კონტროლს ინფორმაციულ აქტივებზე არაავტორიზებული წვდომის, ჩარევის, დატაცებისა ან დაზიანების თავიდან ასაცილებლად.
2. სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ფიზიკური, ტექნიკური, პროცედურული და გარემოს უსაფრთხოების კონტროლის მექანიზმებით.
3. სკოლა ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის და/ან მგრძნობელობის ინფორმაციას. ასეთი მოწყობილობები განთავსებული უნდა იქნეს ფიზიკურად დაცულ ადგილას.

მუხლი 7. სისტემების დაგეგმვა და დანერგვაზე თანხმობა

ახალი სისტემების დაგეგმვისა და დანერგვის პროცესში გათვალისწინებულ უნდა იქნეს სისტემების ტექნიკური და ფუნქციური შესაძლებლობები, რათა არ მოხდეს კრიტიკული სისტემების გამართული მუშაობის შეფერხება.

მუხლი 8. საზიანო პროგრამებზე კონტროლი და უსაფრთხოება

1. საზიანო ან თაღლითური პროგრამების გამოყენების თავიდან აცილების მიზნით აუცილებელია კრიტიკულ სისტემებზე კონტროლის განხორციელება.
2. კრიტიკულ სისტემებში სიახლეების და/ან ცვლილებების დანერგვამდე მოსწავლეების, პერსონალის და მესამე პირთა მიერ შექმნილმა პროგრამულმა პროდუქტებმა ინფორმაციული უსაფრთხოების რისკების შესაბამისად უნდა გაიაროს დეტალური შემოწმება.
3. სკოლის შენობა აღჭურვილი უნდა იყოს ვიდეო სათვალთვალო კამერებით, რომლებიც მოახდენენ დაკვირვებას 24 (ოცდაოთხი) საათის განმავლობაში.
4. პერიოდულობით უნდა ხდებოდეს აპარატურული უზრუნველყოფის დიაგნოსტიკა და საჭიროების შემთხვევაში მათი პროგრამული განახლება.

მუხლი 9. ვირუსებისგან დაცვა

1. სკოლა ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება სკოლის შიგნით და სკოლის მიზეზით – მის გარეთ;
2. სკოლის ყველა კომპიუტერზე დაინსტალირებული უნდა იყოს უახლესი ვერსიის ოპერაციული სისტემა, ხოლო გარე წვდომისგან და ვირუსებისგან დაცვისაგან სისტემაში ჩაშენებული უნდა იყოს ანტივირუსი.
3. მოსწავლეებს არ უნდა ჰქონდეთ წვდომა კომპიუტერების ადმინისტრაციული მართვის უფლებებთან.

მუხლი 10. არქივირება

უნდა განხორციელდეს საარქივო მასალის უსაფრთხოდ შენახვა და მართვა.

მუხლი 11. კომპიუტერული ქსელის მართვა

კომპიუტერული ქსელის (მათ შორის, უკაბელო) ექსპლუატაციაში გაშვების, მხარდაჭერისა და ადმინისტრირებისათვის უნდა ზრუნავდეს საინფორმაციო მენეჯერი.