დამტკიცებულია :

სსიპ კოლეჯ ,,ოპიზარის“ დირექტორის

ბრძანებით

სსიპ კოლეჯ „ოპიზარის“ IT რისკების მართვის პოლიტიკის, ინფორმაციული ინფრასტრუქტურისა და IT პროცესების სისტემის ეფექტურად მართვის წესი

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს სსიპ კოლეჯ „ოპიზარის“ (შემდგომში - კოლეჯის) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, რომელიც უზრუნველყოფს კოლეჯის ყველა პროცესის ეფექტურ მართვას: ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს, კოლეჯის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში მართვის ელექტრონული სისტემა eFlow, ejournal , evet.emis.ge, ადმინისტრირებისა და გამოყენების წესებს. ამასთან კოლეჯი საინფორმაციო პლატფორმების საშუალებით (office 365) Google, Facebook, Zoom, TEAMS უზრუნველყოფს პროფესიულ სტუტენტთა/მსმენელთა და პერსონალის ერთიან საკომუნიკაციო სივრცეს.

2. წინამდებარე წესის დაცვა სავალდებულოა ყველა იმ პირისთვის, რომლებიც თავის ადმინისტრაციულ, აკადემიურ თუ პროფესიული სტუდენტის/მსმენელის საქმიანობაში იყენებს კოლეჯის ინფორმაციულ ტექნოლოგიებსა და რესურსებს .

3. კოლეჯის საინფორმაციო ტექნოლოგოების მომხმარებელი (შემდეგში - მომხმარებელი) ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები: ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

თავი 1 - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს კოლეჯის (შემდგომში – კოლეჯში) ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.

2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:

ა) კოლეჯის IT ინფრასტრუქტურა;

ბ) კოლეჯში არსებული კრიტიკული ინფორმაციული რესურსი, მათშორის პერსონალური მონაცემები;

გ) პირები, რომლებიც იყენებენ ინფორმაციულ სისტემებს ან ახორციელებენ მის ადმინისტრირებას;

დ) პირები, რომლებიც ახორციელებენ ძირითადი მონაცემებისა და ინფორმაციის მართვას

3. პოლიტიკა განსაზღვრავს:

ა) კოლეჯის კრიტიკული ინფორმაციული რესურსის დაცულობას, კონფიდენციალურობას, მთლიანობას და ხელმისაწვდომობას.

ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 3. საინფორმაციო ტექნოლოგების ინფრასტრუქტურის შესაბამისობა კოლეჯში მიმდინარე პროცესებთან და ფიზიკური უსაფრთხოება

1.კოლეჯის საინფორმაციო ტექნოლოგიების ინფრასტრუქტურა მოიცავს კომპიუტერულ ტექნიკას, ქსელს, უსაფრთხოების კამერებს . კომპიუტერულ ტექნიკას კოლეჯი იყენებს როგორც მართვით, ასევე სასწავლო პროცესის მიზნებისათვის. დაწესებულება აღჭურვილია ადმინისტრაციული და სასწავლო პროცესისათვის საკმარისი, სათანადო პარამეტრების მქონე კომპიუტერების რაოდენობით, რომელიც პერიოდულად განახლებადია. კოლეჯის კომპიუტერული ტექნიკა ინტერნეტში ჩართულია 24/7 რეჟიმით, როგორც პერსონალისათვის განკუთვნილ სამუშაო ოთახებში, ასევე სასწავლო პროცესისათვის განკუთვნილ სასწავლო სახელოსნოებში, ბიბლიოთეკის სამკითხველო დარბაზში, აუდიტორიებში, კომპიუტერულ კლას კაბინეტებში და სხვ.

2. ინფორმაციული ტექნოლოგიების სპეციალისტი პერიოდულად საკუთარი ინიციატივით, ან მომხმარებელთა მოთხოვნის საფუძველზე ახორციელებს კოლეჯის კომპიუტერული ტექნიკის, პერიფერიული მოწყობილობების მდგომარეობის შესწავლას (როგორც ტექნიკურ, ასევე პროგრამულ დონეზე), მათ შესაბამისობას კოლეჯში მიმდიწარე პროცესებთან და საჭიროების შემთხვევაში იღებს გადაწყვეტილებას მათი შეკეთების/ახლით ჩანაცვლების შესახებ.

3. კოლეჯის მთელ პერიმეტრზე, მათ შორის ბიბლიოთეკაში, ჰოლში, დერეფნებში, საკონფერენციო დარბაზში, უზრუწველყოფილია უსადენო წვდომის ქსელით (Wifi). უსადენო ქსელის მართვას, მის უსაფრთხოებასა და დაცულობას (როგორც ტექნიკურ, ასევე პროგრამულ დონეზე) ახორციელებს ინფორმაციული ტექნოლოგიების სპეციალისტი.

4. კოლეჯს ინტერნეტ მომსახურებას უწევს ინტერნეტ-პროვაიდერი, რომელთანაც კოლეჯს გაფორმებული აქვს ხელშეკრულება.

5. კოლეჯი ახორციელებს კონტროლს ინფორმაციულ აქტივებზე არაავტორიზებული წვდომის, ჩარევის, დატაცებისა ან დაზიანების თავიდან ასაცილებლად.

6. კოლეჯი ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის და/ან მგრძნობელობის ინფორმაციას. ასეთი მოწყობილობები განთავსებულია ფიზიკურად დაცულ ადგილას.

მუხლი 4. ინფორმაციული უსაფრთხოების ინციდენტები

1. კოლეჯი ვალდებულია განახორციელოს უსაფრთხოების ინციდენტების იდენტიფიცირება, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას.
2. კოლეჯის ინფორმაციული ტექნოლოგიების სისტემის ფუნქციონირებაზე პასუხისმგებელი პირი/პირები წარმოადგენენ ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების (ინციდენტის დადგომის შემთხვევაში), მათი წყაროების (შიდა, გარე) მათი ფორმების (DDoS, Keylog და სხვა) მიხედვით, გამოსწორებისა და ოპტიმიზაციის რეკომენდაციებთან ერთად

მუხლი 5. კომუნიკაციებისა და ოპერაციების მართვა

1. კოლეჯი ახორციელებს მუდმივ კონტროლს ინფორმაციის დამამუშავებელ მოწყობილობებზე მათი სწორი და უსაფრთხო სარგებლობის უზრუნველყოფის მიზნით.

მუხლი 6. ახალი სისტემის დაგეგმვა შემუშავება

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

მუხლი 7. საზიანო პროგრამებზე კონტროლი

1. საზიანო ან თაღლითური პროგრამების გამოყენების თავიდან აცილების მიზნით აუცილებელია კრიტიკულ სისტემებზე კონტროლის განხორციელება.

მუხლი 8. ვირუსებისგან დაცვა

1.კოლეჯში მოწყობილია ზოგადი სტანდარტის შესაბამისი ქსელი (Router -> ვარსკვლავური ტოპოლოგიის ლოკალური ქსელი). საკაბელო ქსელით დაფარულია კოლეჯის მთელი ტერიტორია.

2. კოლეჯის ყველა კომპიუტერი აღჭურვილია ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ რეკომენდირებული და დაყენებული ანტივირუსული პროგრამული უზრუნველყოფით. ანტივირუსული ბაზების განახლება ხორციელდება სისტემატურად.

3. უსადენო ქსელის ყველა წერტილი დაცულია უსაფრთხოების შიფრით.

4. კოლეჯის ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ კომპიუტერული ქსელის მონიტორინგი ხორციელდება ყოველდღიურად.

5. ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება პერმანენტულად.

მუხლი 9. კომპიუტერული ქსელის მართვა

1. კომპიუტერული ქსელის მართვა ხორციელდება ინფორმაციული ტექნოლოგიების სპეციალისტის მიერ. ინფორმაციული ტექნოლოგიების სპეციალისტი განსაზღვრავს რიგ შეზღუდვებსა და დაშვებებს უსაფრთხოების პოლიტიკიდან გამომდინარე. შეზღუდვები და დაშვებები ვებსაიტებსა თუ სხვა ინფორმაციულ რესურსზე ფორმირდება კოლეჯის დირექციასთან შეთანხმებით და კოლეჯის რეგულაციების (პერსონალური მონაცემთა დაცვის წესი) გათვალისწინებით.

მუხლი 10. სისტემების უსაფრთხოება ტესტირებისა და შექმნის პროცესში

1. სისტემების ტესტირება ხდება იზოლირებულ გარემოში, რათა სასიცოცხლოდ მნიშვნელოვანი კრიტიკული სისტემები დაცულ იქნეს შეცდომით განადგურების და/ან დაზიანებისაგან.

2. სტრატეგიამ და მისმა ფუნქციონირებამ უნდა უზრუნველყოს კოლეჯის ინფორმაციის დამუშავების პროცესში მოულოდნელი წყვეტის რისკის შემცირება და მოახდინოს მისი დროული აღდგენა.

3. ძირითადი როუტერის მწყობრიდან გამოსვლის შემთხვევაში ხდება ხარვეზის გამოსწორებაზე დაუყონებლივი რეაგირება.

თავი II - კოლეჯის სასწავლო პროცესის მართვის ელექტრონული სისტემა

მუხლი 11. სასწავლო პროცესის მართვის სისტემის აღწერა

1. კოლეჯის სასწავლო პროცესის მართვის სისტემა eFlow, evet.emis.ge უზრუნველყოფს კოლეჯის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას, არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.

2. სისტემის ზოგადი ფუნქციები:

ა) კოლეჯში სასწავლო პროცესის მართვის ავტომატიზაცია;

ბ) ფინანსური მოდულის ავტომატიზაცია;

გ) ელექტრონული საქმის წარმოება

3. სისტემაში გამოყენებულია კრიპტოგრაფია, სადაც დაშიფრულია მომხმარებლების (ადმინისტრაცია, პროფესიული განათლების მასწავლებელი) პაროლები.

4. სისტემის მომხმარებლებია:

ა) დირექცია;

ბ) ადმინისტრაცია;

გ) პროფესიული განათლების მასწავლებელი;

დ) ტექნიკური პერსონალი

მუხლი 12. განვითარების მექანიზმები

1. კოლეჯში არსებული ქსელის ინფრასტრუქტურა მოწყობილია თანამედროვე სტანდარტებით, კოლეჯი მუდმივად ზრუნავს სტანდარტების ცვლილების შემთხვევაში შესაბამისობაში მოიყვანოს თავისი ინფრასტრუქტურა ახალ სტანდარტთან.

2. კოლეჯი უზრუნველყოფს საინფორმაციო რესურსების განვითარებას და გაუმჯობესებას

მუხლი 13 . დასკვნითი დებულებანი

1 .წინამდებარე წესის დამტკიცება , ცვლილებების ან/და დამატებების შეტანა ხორციელდება კოლეჯის დირექტორის ინდივიდუალურ-ადმინისტრაციული სამართლებრივი აქტით.