დანართი 1

დამტკიცებულია:
ა(ა)იპ კოლეჯი „იკაროსის“ დირექტორის
2020 წლის 27 აგვისტოს N01-09/176 ბრძანებით

ა(ა)იპ კოლეჯის “იკაროსი” IT რისკების მართვის პოლიტიკისა და საინფორმაციო ინფრასტრუქტურისა და IT პროცესების სისტემის ეფექტიანობის პოლიტიკა

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს ა(ა)იპ კოლეჯის „იკაროსი“ (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, emis ადმინისტრირებისა და გამოყენების წესებს. ამასთან კოლეჯი საინფორმაციო პლატფორმების საშუალებით (Icarus.edu.ge. Gmail, Facebook და სხვა) უზრუნველყოფს პროფესიულ სტუდენტთა/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 ტექნოლოგიების მომხმარებელი (შემდეგში - მომხმარებელი) ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები: ინტეელქტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

თავი 1 - ინფორმაციული ტექბოლოგიების მართვის პოლიტიკა

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს კოლეჯის ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.
2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:
ა) კოლეჯის IT ინფრასტრუქტურა
ბ) კოლეჯში არსებული ძირითადი მონაცემები და ინფორმაცია, მათშორის პერსონალურ მონაცემთა დაცვა
გ) პირები, რომლებიც იყენებენ ინფორმაციულ სისტემებს ან ახორციელებენ მის ადმინისტრირებას
დ) პირები, რომლებიც ახორციელებენ ძირითადი მონაცემებისა და ინფორმაციის მართვას
3. პოლიტიკა განსაზღვრავს:
ა) კოლეჯის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;
ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 3. ფიზიკური უსაფრთხოება

1. კოლეჯი 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. 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 პირები პერიოდულად წარმოადგენენ ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების, მათი წყაროების (შიდა, გარე) მათი ფორმების (DDoS, Keylog და სხვა) მიხედვით, გამოსწორებისა და ოპტიმიზაციის რეკომენდაციებთან ერთად.

მუხლი 5. კომუნიკაციებისა და ოპერაციების მართვა

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

მუხლი 6. ახალი სისტემის დაგეგმვა შემუშავება

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

მუხლი 7. საზიანო პროგრამებზე კონტროლი

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

მუხლი 8. ვირუსებისგან დაცვა

1. კოლეჯი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება კოლეჯის შიგნით და კოლეჯის მიზეზით – მის გარეთ, სისტემები, აპლიკაციები და მონაცემთა სარეზერვო ასლები.
2. ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება პერმანენტულად.

მუხლი 9. კომპიუტერული ქსელის მართვა

1. კოლეჯში, როგორც ფიზიკურ, ასევე უკაბელო ქსელში ჩართულ იმ კომპიუტერებს და მოწყობილებებს, რომლებიც განეკუთნებიან კოლეჯის აქტივებს, როუტერი ანიჭებს წინასწარ შერჩეულ IP მისამართს.
2. ისეთი მოწყობილობები, რომლებიც არ განეკუთნებიან კოლეჯის აქტივებს და იყენებენ კოლეჯის უკაბელო ქსელს (wifi), სარგებლობენ სპეციალური გამოყოფილი ქსელით.

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 დაუყოვნებლივი რეაგირება.

თავი II - კოლეჯის სასწავლო პროცესის მართვის ელექტრონული სისტემა

მუხლი 11. სასწავლო პროცესის მართვის სისტემის აღწერა

1. კოლეჯის სასწავლო პროცესის მართვის სისტემა eFlow, emis უზრუნველყოფს კოლეჯის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.
2. სისტემის ზოგადი ფუქნციები:
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 მომხმარებლები არიან:
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, გაუმჯობესებას და პროცესების ოპტიმიზაციასა და მონიტორინგს, როგორც ადმინისტრაციაში პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუთსორსინგით.