დანართი №4
დამტკიცებულია შპს ავიცენას საერთაშორისო საზოგადოებრივი
კოლეჯის დირექტორის 2024 წლის ---------- N ----------ბრძანებით

შპს ავიცენას საერთაშორისო საზოგადოებრივი კოლეჯის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

თბილისი 2024

მუხლი 1.

1. წინამდებარე დოკუმენტი განსაზღვრავს შპს ავიცენას საერთაშორისო საზოგადოებრივი კოლეჯის (შემდგომში - კოლეჯი) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს კოლეჯის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში.
2. წინამდებარე დოკუმენტის შესაბამისი ნაწილების დაცვა სავალდებულოა ყველა იმ პირისთვის, რომლებიც თავის საქმიანობაში იყენებს კოლეჯის ინფორმაციულ ტექნოლოგიებსა და რესურსებს.
3. კოლეჯის საინფორმაციო ტექნოლოგიების მომხმარებელი (შემდეგში - მომხმარებელი) ვალდებულია დაიცვას საქართველოს კანონმდებლობითა და კოლეჯის მიერ დადგენილი მოთხოვნები ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

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 ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა;
ბ) კოლეჯში არსებული ძირითადი მონაცემები და ინფორმაცია
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 პირი პერიოდულად წარმოადგენს ანგარიში და რეკომენდაციები ინფორმაციული უსაფრთხოების ინციდენტების წყაროების (შიდა, გარე) შესახებ.

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 სისტემების გამართული 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. კოლეჯი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება კოლეჯის შიგნით და კოლეჯის მიზეზით – მის გარეთ;
2. ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება სინქრონულად კოლეჯის google drive - ზე.

მუხლი 9. კომპიუტერული ქსელის მართვა

1. კოლეჯში როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილებების mac მისამართები რომლებიც განეკუთნებიან კოლეჯის აქტივებს წინასწარ არის გაწერილი როუტერში, რომელიც ანიჭებს წინასწარ შერჩეულ Ip მისამართს.
2. ისეთი მოწყობილობები, რომლებიც არ განეკუთნებიან კოლეჯის აქტივებს და იყენებენ კოლეჯის უკაბელო ქსელს (wifi), სარგებლობენ სპეციალური გამოყოფილი ქსელით, რომლის საშუალებითაც შეუძლიათ წვდომა ჰქონდეთ მხოლოდ დაშვებულ ვებ გვერდების კატეგორიასთან, რომლებიც წინასწარ შერჩეულია.

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. კოლეჯმა უნდა უზრუნველყოს ინფორმაციის დამუშავების პროცესში მოულოდნელი წყვეტის რისკის შემცირება და მოახდინოს მისი დროული აღდგენა.
3. ძირითადი როუტერის მწყობრიდან გამოსვლის შემთხვევაში ხდება სარეზერვო როუტერის ჩართვა, შედეგის დადგომიდან 10 წუთის განმავლობაში.

მუხლი 11. სასწავლო პროცესის მართვის სისტემის აღწერა

1. სასწავლო პროცესის მართვის სისტემა უზრუნველყოფს საგანმანათლებლო და ადმინისტრაციულ საქმიანობას, არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციას დამუშავებასა და დაცვას.
2. სისტემის ზოგადი ფუქნციები:
ა) სასწავლო პროცესის მართვის ავტომატიზაცია
ბ) ფინანსური მოდულის ავტომატიზაცია
გ) ელექტრონულ საქმის წარმოება

3. სისტემაში გამოყენებულია კრიპტოგრაფია სადაც დაშიფრულია მომხმარებლების (ადმინისტრაცია, მასწავლებელი, პროფესიული სტუდენტი) პაროლები.
4. სისტემის მომხმარებლებია:
ა) ადმინისტრაცია
ბ) მასწავლებელი
გ) პროფესიული სტუდენტი

მუხლი 12. სისტემის უსაფრთხოება

1. სისტემის კოდი იწერება სპეციალურად გამოყოფილ ლოკალურ სერვერზე, სადაც ხდება სისტემაში დამატებული ახალი მოდულის ტესტირება შემდეგ ხდება შემოწმებული კოდის ატვირთვა ძირითად სერვერზე
2. სერვერზე ინახება მოქმედებათა ლოგები, შემდეგი მონაცემებით: მოქმედების ავტორი, მოქმედების დრო, შესრულებული მოქმედება, IP მისამართი
3. ბიზნესის უწყვეტობის მიზნით, ძირითადი სერვერის მწყობრიდან გამოსვლის შემთხვევაში, ავტომატურად ირთვება სარეზერვო სერვერი, რომელიც ახდენს რეპლიკაციას ძირითად სერვერთან.
4. სისტემის მონაცემები დღეში ერთხელ ავტომატურად ინახება კოლეჯის google drive ზე.

მუხლი 13. განვითარების მექანიზმები

1. კოლეჯში არსებული ქსელის ინფრასტრუქტურა მოწყობილია თანამედროვე სტანდარტებით, კოლეჯი მუდმივად ზრუნავს სტანდარტების ცვლილების შემთხვევაში შესაბამისობაში მოიყვანოს თავისი ინფრასტრუქტურა ახალ სტანდარტთან.
2. არსებული სასწავლო პროცესის მართვის სისტემის კოდი იწერება არსებული სტანდარტებით, სტანდარტების ცვლილებასთან ერთად იცვლება პროგრამული უზრუნველყოფის მიდგომა და მისი გადაჭრის გზები.
3. კოლეჯი უზრუნველყოფს საინფორმაციო რესურსების განვითარებას, გაუმჯობესებას და პროცესების ოპტიმიზაციისა და მონიტორინგს, როგორც ადმინისტრაციაში პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუთსორსინგით.