დანართი
დამტკიცებულია ა(ა)იპ კოლეჯი ,,ჰორიზონტი“-ს
დირექტორის 2021 წლის 31 იანვრის N 04-4 ბრძანებით

ა(ა)იპ კოლეჯის „ ჰორიზონტი“ IT რისკების მართვის პოლიტიკა

მუხლი 1. 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს ა(ა)იპ კოლეჯის “ჰორიზონტი” (შემდგომში - კოლეჯის) ინფორმაციული ტექნოლოგიის რისკების 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 გამოყენების წესებს. ამასთან კოლეჯი საინფორმაციო პლატფორმების საშუალებით (http://horizonti.ge, Gmail, Facebook და TEAMS, ZOOM) 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: ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

   დოკუმენტში გათვალისწინებულია ის თავისებურებები, რომლებიც აუცილებელია ინფორმაციული უსაფრთხოების რისკების მართვის პოლიტიკის ჩამოსაყალიბებლად და შემუშავებულია რეკომენდაციები, ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირების, შეფასების, მოპყრობის მეთოდების შესახებ.

2. ზოგადი ინფორმაცია

ინფორმაციული უსაფრთხოების რისკების მართვა უწყვეტი პროცესია. ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

- რისკების იდენტიფიცირებას;
- რისკებთან მოპყრობის პრიორიტეტულობის დადგენას;
- რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას;
- რისკების მართვასთან დაკავშირებული გადაწყვეტილებების მიღებაში ჩართული დაინტერესებული პირების ინფორმირებულობას რისკების მართვის სტატუსის შესახებ;

- რისკებთან მოპყრობის მონიტორინგის ეფექტიანობას;
- რისკების მართვისადმი მიდგომის გაუმჯობესების მიზნით საჭირო ინფორმაციის შეგროვებას;
- მენეჯერებისა და თანამშრომლების ინფორმირებულობას რისკებისა და მათი შემცირების შესახებ.

ინფორმაციული უსაფრთხოების რისკები მართვის პროცესი შედგება შემდეგი პროცესებისგან: ორგანიზაციული გარემოს დადგენა, რისკების შეფასება, რისკებთან მოპყრობა, რისკების მიღება, რისკების შესახებ ინფორმირება და რისკების მონიტორინგი და განხილვა.

რისკებთან მოპყრობის ეფექტიანობა დამოკიდებულია რისკის შეფასების შედეგებზე. ინფორმაციული უსაფრთხოების რისკების მართვის მთელი პროცესის განმავლობაში მნიშვნელოვანია, რომ არსებობდეს კომუნიკაცია რისკებსა და მათთან მოპყრობას შორის, ასევე შესაბამის მენეჯერებსა და თანამშრომლებს შორის. მენეჯერებისა და თანამშრომლების ინფორმირებულობა ორგანიზაციის რისკების შესახებ, რისკების და პრობლემური საკითხების შემცირების კონტროლის მექანიზმის შესახებ ხელს უწყობს ინციდენტების და მოულოდნელი შემთხვევების ეფექტურ აღმოფხვრას.

თავი I - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა უზრუნველყოფს კოლეჯის ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.

2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დაცვის სფეროებს წარმოადგენს:

ა) კოლეჯის IT ინფრასტრუქტურა;

ბ) კოლეჯში არსებული ძირითადი მონაცემები და ინფორმაცია, მათ შორის პერსონალური მონაცემთა დაცვა;

3. ინფორმაციული ტექნოლოგიების მართვის 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.

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 ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების, მათი წყაროების (შიდა, გარე) 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. საზიანო პროგრამებზე კონტროლი

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

მუხლი 7. ვირუსებისგან დაცვა

1. კოლეჯი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება კოლეჯის შიგნით და კოლეჯის მიზეზით – მის გარეთ, სისტემები, აპლიკაციები.

მუხლი 8. კომპიუტერული ქსელის მართვა

1. კოლეჯში, როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილებების mac მისამართები რომლებიც განეკუთნებიან კოლეჯის აქტივებს წიანსწარ არის გაწერილი როუტერში, რომელიც ანიჭებს წინასწარ შერჩეულ **Ip** მისამართს.

2. ისეთი მოწყობილობები, რომლებიც არ განეკუთნებიან კოლეჯის აქტივებს და იყენებენ კოლეჯის უკაბელო ქსელს **(wi fi),** სარგებლობენ სპეციალური გამოყოფილი ქსელით.

მუხლი 9. ახალი სისტემის დაგეგმვა შემუშავება

1. სისტემების დაგეგმვისა და დანერგვის პროცესში ხდება სისტემების ტექნიკური და ფუნქციური შესაძლებლობების გათვალისწინება, რათა არ მოხდეს კრიტიკული სისტემების გამართული მუშაობის შეფერხება.

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**, emis უზრუნველყოფს კოლეჯის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას, არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.

2. სისტემის ზოგადი ფუნქციებია:

ა) კოლეჯში სასწავლო პროცესის მართვის ავტომატიზაცია

ბ) ფინანსური მოდულის ავტომატიზაცია

გ) ელექტრონულად საქმისწარმოება.

მუხლი 12. განვითარების მექანიზმები

1. კოლეჯი მუდმივად ზრუნავს, რომ ინფრასტრუქტურა შესაბამისობაში ჰქონდეს სტანდარტებთან. კოლეჯში არსებული ქსელის ინფრასტრუქტურა შეესაბამება თანამედროვე სტანდარტების მოთხოვნებს.

2. კოლეჯი უზრუნველყოფს საინფორმაციო რესურსების განვითარებასა და გაუმჯობესებას.

დირექტორი: ნანა ჯოლია