



სსიპ - ილია წინამძღვრიშვილის სახელობის კოლეჯი
საინფორმაციო ინფრასტრუქტურისა და IT პროცესების სისტემების ეფექტიანობისა და IT
რისკების მართვის პოლიტიკა

თავი I. ზოგადი დებულებები

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს სსიპ ილია წინამძღვრიშვილის სახელობის კოლეჯის (შემდგომში - კოლეჯის) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, რომლის მიზანია კოლეჯმა უზრუნველყოს ერთიანი პრინციპით მოქმედი, უსაფრთხო და ეფექტიანი ელექტრონული სერვისების ხელმისაწვდომობა როგორც სასწავლო, ასევე ადმინისტრაციული ნაწილისთვის სათანადო ინფრასტრუქტურის გამოყენებით.
2. დოკუმენტი მოიცავს ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს, კოლეჯის ელექტრონულ დოკუმენტრუნვისა და საკომუნიკაციო სისტემებს.
3. წინამდებარე დოკუმენტის მიხედვით განსაზღვრული წესები ვრცელდება კოლეჯის ყველა ფილიალზე და დაცვა სავალდებულოა ყველა იმ პირისთვის (ადმინისტრაცია, პროფესიული განათლების მასწავლებლები, პროფესიული სტუდენტები/მსმენელები), რომელიც თავის საქმიანობაში იყენებს კოლეჯის ინფორმაციულ ტექნოლოგიებსა და რესურსებს.
4. კოლეჯის საინფორმაციო ტექნოლოგიების მომხმარებელი (შემდგომში - მომხმარებელი) ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები: ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

თავი II - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მუხლი 2. პასუხისმგებელი პირები

1. დაწესებულება ვალდებულია უზრუნველყოს კომპიუტერული ტექნიკის გამართულ/მუშა მდგომარეობაში არსებობა და კომუნიკაციის საშუალების, ინტერნეტ-რესურსების ხელმისაწვდომობა თანამშრომლებისა და პროფესიული სტუდენტების/მსმენელებისათვის.
2. კომპიუტერული ტექნიკის გამართულ მუშაობაზე, პროგრამულ უზრუნველყოფაზე, არსებული პრობლემების დროულად მოგვარებაზე, ქსელის მართვაზე და უსაფრთხოებაზე პასუხისმგებელი პირი არის ქსელების ადმინისტრატორი.

მუხლი 3. აპარატურის ფიზიკური უსაფრთხოება

1. კოლეჯი ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მალალი კრიტიკულობის და/ან მგრძობელობის ინფორმაციას. აღნიშნული მოწყობილობები განთავსებულია ფიზიკურად დაცულ ადგილას - სასერვერო ოთახში.
2. სასერვერო ოთახებში დაცულია ფიზიკური უსაფრთხოება და ხდება დაშვების კონტროლი.
3. სასერვერო ოთახში დაშვება აქვს ქსელების ადმინისტრატორს- სხვა პირებისთვის სასერვერო ოთახში შესვლა შესაძლებელია მხოლოდ ქსელების ადმინისტრატორის ნებართვით.
4. კოლეჯის კომპიუტერული ტექნიკით და რესურსებით სარგებლობა შეუძლია დაწესებულების თანამშრომლებს და პროფესიულ სტუდენტებს/მსმენელებს. ნებართვის გარეშე დაუშვებელია მესამე პირების მიერ დაწესებულების კომპიუტერული ტექნიკითა და რესურსებით სარგებლობა.

5. კომპიუტერული ტექნიკის დაზიანების ან პროგრამული ხარვეზის შემთხვევაში, თითოეული თანამშრომელი ვალდებულია დაუყოვნებლივ აცნობოს პრობლემა დაწესებულების კომპიუტერული ქსელის ადმინისტრატორს.
6. კომპიუტერული ტექნიკის დაზიანების ან პროგრამული ხარვეზის შემთხვევაში, პროფესიული სტუდენტი/მსმენელი ვალდებულია დაუყოვნებლივ აცნობოს პრობლემა პროფესიული განათლების მასწავლებელს ან კოლეჯის ადმინისტრაციას.
7. დაწესებულების საოფისე/სასწავლო აუდიტორიის კომპიუტერული ტექნიკის დაკარგვის შემთხვევაში შესაბამისი პასუხისმგებელი პირი ვალდებულია დაუყოვნებლივ აცნობოს დირექტორს ან მისი არყოფნის დროს შესაბამის პასუხისმგებელ პირებს.
8. აკრძალულია ნებართვის გარეშე კომპიუტერული და სხვა საკომუნიკაციო ტექნიკის დემონტაჟი და სხვა ადგილას გადატანა. ასევე, კომპიუტერის ან მისი რომელიმე ნაწილის სხვა პირზე გადაცემა და კომპიუტერზე დამატებითი, შიდა და პერიფერიული მოწყობილობების მიერთება პასუხისმგებელი პირის ნებართვის გარეშე.
9. დაწესებულების თანამშრომლები და პროფესიულ სტუდენტები/მსმენელები ვალდებული არიან არ დააზიანონ დაწესებულების ტექნიკა და ინვენტარი, გამოყენების შემდეგ გამორთონ კომპიუტერები და დაიცვან სანიტარულ-ჰიგიენური ნორმები კომპიუტერულ ტექნიკასთან მუშაობის დროს.

მუხლი 4. ინფორმაციაზე წვდომის პოლიტიკა

1. კოლეჯი ახორციელებს კონტროლს ინფორმაციულ აქტივებზე არაავტორიზებული წვდომის, ჩარევის, დატაცებისა ან დაზიანების თავიდან ასაცილებლად.
2. მომხმარებლები არ უნდა შეეცადონ კოლეჯის ინფორმაციული ტექნოლოგიების სისტემებზე უნებართვო წვდომის მოპოვებას.
3. ინფორმაციის გადაცემა ხდება მხოლოდ ლეგიტიმური და უფლებამოსილი მომხმარებლებისთვის როგორც კოლეჯის შიგნით ისე კოლეჯის გარეთ.
4. ყველა მომხმარებელს, ვისაც სჭირდება კოლეჯში არსებულ კომპიუტერულ სისტემებზე წვდომა, უნდა ჰქონდეს ლეგიტიმური მომხმარებლის სახელი და პაროლი.
5. თითოეული მომხმარებლებისთვის მინიჭებული უნდა იყოს შესაბამისი პრივილეგია.
6. პაროლებთან მიმართებაში კოლეჯის ყველა თანამშრომელი ვალდებულია:
 - 6.1 ნებისმიერი დროებითი პაროლი შეცვალოს გამოყენებისთანავე;
 - 6.2 პაროლში გამოიყენოს მინიმუმ 8 სიმბოლო (სასურველია დიდი ასოს, პატარა ასოს და რიცხვის კომბინაცია);
 - 6.3 არ ჩაიწეროს პაროლები ან არ გაამჟღავნოს სხვა პირებთან;
 - 6.4 ელექტრონული ფოსტით კომუნიკაციისას არ გაგზავნოს პაროლი ღია ტექსტის სახით;
 - 6.5 მომხმარებლები თვითონ არიან პასუხისმგებლები საკუთარი პაროლების უსაფრთხოებაზე და საიდუმლოებაზე.
7. პაროლების გაზიარება ჩაითვლება აღნიშნული პოლიტიკის დარღვევად და შესაძლოა გამოიწვიოს დისციპლინური პასუხისმგებლობის ზომების მიღება.
8. დაუყოვნებლივ უნდა მოხდეს იმ თანამშრომლის მომხმარებლების ანგარიშის დაბლოკვა, რომელმაც დატოვა სამსახური.
9. ნებისმიერი ინციდენტი, რომელიც ეხება კოლეჯის ინფორმაციული ტექნოლოგიების სისტემებზე არაავტორიზებულ წვდომას, დაუყოვნებლივ უნდა ეცნობოს ინფორმაციის ტექნოლოგიების უსაფრთხოებაზე პასუხისმგებელ პირს.
10. კოლეჯი აფასებს ნებისმიერ ინციდენტს და უზრუნველყოფს შესაბამისი ტექნიკური და პროცედურული ზომების გატარებას გამოვლენილი სისუსტეების აღმოსაფხვრელად.

მუხლი 5. პროგრამული უზრუნველყოფის პოლიტიკა

1. კოლეჯში ყველა პროგრამული ინსტალაცია ხდება უსაფრთხოდ და ლეგიტიმურად.
2. ოპერაციული სისტემებისა და პროგრამების განახლება შეუძლია მხოლოდ უფლებამოსილ პირებს.
3. პროგრამული უზრუნველყოფისას ინფორმაციის დაზიანებასთან და დაკარგვასთან დაკავშირებული რისკები მინიმუმამდეა დაყვანილი.
4. კომპიუტერებში დაინსტალირებულია ანტივირუსული უზრუნველყოფა და ოპერაციული სისტემები დაცულია მავნე კოდის მქონე პროგრამებისგან (worm, trojan, ransomware) და ვირუსებისგან.
5. საჭიროების შემთხვევაში, მნიშვნელოვანი მონაცემების დაკარგვის პრევენციისთვის ახდენს რეზერვაციას (Backup).
6. პასუხისმგებელ პირთან შეთანხმების გარეშე აკრძალულია კომპიუტერული პროგრამების ინსტალაცია, გასართობი და სხვა არა სასწავლო, არა საგანმანათლებლო რესურსების გამოყენება, რაც არ არის დაკავშირებული დაწესებულების პერსონალის სამუშაოსთან ან/და საგანმანათლებლო საქმიანობასთან.
7. აკრძალულია აუდიო და ვიდეო ფაილების გადმოწერა, რომელიც არ არის დაკავშირებული სასწავლო პროცესთან ან დაწესებულების საქმიანობის სფეროსთან.
8. ყველა მომხმარებელი ვალდებულია გაუხსნელად წაშალოს საეჭვო, უცნობი გამომგზავნის მიღებული ელექტრონული ფოსტა ან/და ფაილი.
9. პროგრამული განახლების ან ახალი პროგრამის შესყიდვა იგეგმება საჭიროების მიხედვით და ხდება უსაფრთხოების რისკების გათვალისწინება.
10. საავტორო უფლებების დარღვევის თავიდან ასაცილებლად და ინფორმაციის დასაცავად, პასუხისმგებელი პირი პერიოდულად მონიტორინგს უწევს კომპიუტერების პროგრამულ უზრუნველყოფას.

მუხლი 6. ქსელის მართვის პოლიტიკა

1. კოლეჯის კომპიუტერული ტექნიკა დაკავშირებულია ერთმანეთთან შიდა ქსელის საშუალებით და დაკავშირებულია ინტერნეტთან.
2. ინტერნეტი წარმოადგენს დაწესებულების საქმიანობის წარმართვისთვის აუცილებელ ინსტრუმენტს. მასთან დაკავშირება შეუძლია კოლეჯის ყველა თანამშრომელს, ყველა პროფესიულ სტუდენტს/მსმენელს და საჭიროების შემთხვევაში, შესაბამისი ნებართვით კოლეჯის ვიზიტორებს.
3. კოლეჯის ქსელს მართავს კოლეჯის ქსელის ადმინისტრატორი.
4. კოლეჯის შიდა ქსელი დაყოფილია ლოგიკურ ქვექსელებად - ადმინისტრაციისთვის და სასწავლო პროცესისთვის. ქვექსელების შორის შეზღუდულია მარშუტიზაცია.
5. კოლეჯი ასევე იყენებს უკაბელო ქსელს (Wi-Fi), რომელიც გამიჯნულია ადმინისტრაციის, პროფესიული სტუდენტების და სტუმრების მიხედვით.
6. კოლეჯის ქსელზე უკაბელო დაკავშირებისას მოწყობილობებმა უნდა დააკმაყოფილონ უსაფრთხოების მითითებული ნორმები, წინააღმდეგ შემთხვევაში შეეზღუდებათ კავშირი.
7. ქსელში ჩართული კომპიუტერები ავტომატურად იღებენ IP მისამართებს, DHCP სერვისის საშუალებით.
8. კოლეჯის ქსელი დაცულია, როგორც ფიზიკური შეტევის, ისე უნებართვო შეჭრისგან.
9. ქსელში არსებულ რესურსებზე წვდომა მკაცრად კონტროლდება, რათა თავიდან იქნას აცილებული არასანქცირებული წვდომა.
10. ქსელური შეტევებისგან თავდასაცავად და პოტენციური რისკების შესამცირებლად კოლეჯი იყენებს სათანადოდ კონფიგურირებულ ბრენდმაუერს(Firewall).
11. ქსელში ჩართული ნებისმიერი პირადი მოწყობილობის მართვაზე პასუხისმგებელია თვითონ მომხმარებელი.

12. გარე ქსელიდან კოლეჯის ინფორმაციულ ტექნოლოგიებზე წვდომა დასაშვებია მხოლოდ VPN-ის გამოყენებით, შესაბამისი ლეგიტიმური მომხმარებლის სახელით და პაროლით.
13. დაწესებულების ინტერესებიდან გამომდინარე, საჭიროების შემთხვევაში პასუხისმგებელ პირს შეუძლია შეზღუდოს ადმინისტრაციის მიერ დაწესებულ ინტერნეტ რესურსებზე წვდომა.
14. აკრძალულია გაცნობის, გასართობი, სათამაშო, აზარტული და მსგავსი ტიპის ვებგვერდების გამოყენება, რომლებიც არ არის პირდაპირ კავშირში დაწესებულების საქმიანობასთან.
15. მასწავლებლებისთვის და სტუდენტებისთვის შეზღუდულია სასწავლო პროცესისთვის შეუსაბამო შინაარსის კონტენტი. ადმინისტრაციის თანამშრონლებისთვის შეზღუდულია გასართობ კონტენტზე წვდომა
16. ნებისმიერი ინციდენტი, რომელიც ეხება კოლეჯის ქსელს დაუყოვნებლივ უნდა ეცნობოს პასუხისმგებელ პირს.
17. კოლეჯის ინფორმაციული ტექნოლოგიების სისტემის ფუნქციონირებაზე პასუხისმგებელი პირი პერიოდულად წარმოადგენს ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების შესახებ (არსებობის შემთხვევაში).

მუხლი 7. ინფორმაციული ტექნოლოგიების სისტემების 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 პროფესიული სტუდენტებისთვის/მსმენელებისთვის კომპიუტერული ტექნიკის აპარატურულ და პროგრამულ განახლებას საგანმანათლებლო პროგრამების საჭიროებების მიხედვით.
3. ტექნოლოგიური განვითარების შესაბამისად, კოლეჯი უზრუნველყოფს ადმინისტრაციის კომპიუტერული ტექნიკის აპარატურულ და პროგრამულ განახლებას კოლეჯის საქმიანობის ეფექტურობის გაზრდისთვის.
4. კოლეჯი რეგულარულად გეგმავს მონაცემების და ინფორმაციული ტექნოლოგიების უსაფრთხოების შესახებ ცნობიერების ამაღლების ღონისძიებებს და ტრენინგებს პერსონალისთვის.
5. საჭიროების მიხედვით კოლეჯი უზრუნველყოფს ახალი ინფორმაციული ტექნოლოგიების სისტემების დანერგვას.
6. ახალი სისტემების დაგეგმვისა და დანერგვის პროცესში გათვალისწინებულ უნდა იქნეს სისტემების ტექნიკური და ფუნქციური შესაძლებლობები, რათა არ მოხდეს კრიტიკული სისტემების გამართული მუშაობის შეფერხება.
7. ახალი სისტემების დანერგვისას კოლეჯი ახდენს ტესტირებას, რათა სამუშაო პროცესში არ გამოიწვიოს ხარვეზები.

თავი III - ელექტრონული სისტემები

მუხლი 8. ელექტრონული საკომუნიკაციო სისტემები

1. ერთიანი საკომუნიკაციო სივრცის შესაქმნელად კოლეჯი იყენებს zoom - ისა და Microsoft Teams-ის პლატფორმას.
2. ადმინისტრაციისთვის, პროფესიული განათლების მასწავლებლებისთვის და პროფესიული სტუდენტებისთვის კოლეჯი იყენებს შესაბამის ანგარიშებს (Account).

მუხლი 9. ელექტრონული დოკუმენტბრუნვის სისტემა

1. კოლეჯი დოკუმენტბრუნვისთვის იყენებს ელექტრონულ სისტემას eFlow (eflow.emis.ge).

2. eFlow-ს საშუალებით კოლეჯი უზრუნველყოფს კოლეჯის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციას დამუშავებასა და დაცვას.
3. eFlow-ს საშუალებით ადმინისტრაციის წარმომადგენლებს და პროფესიული განათლების მასწავლებლებს აქვთ ოფიციალური კომუნიკაცია.
4. eFlow სისტემის ზოგადი ფუნქციები:
 - 4.1 კოლეჯში სასწავლო პროცესის მართვის ავტომატიზაცია;
 - 4.2 ფინანსური მოდულის ავტომატიზაცია;
 - 4.3 ელექტრონულ საქმის წარმოება.
5. eFlow სისტემის მომხმარებლები:
 - 5.1 დირექცია;
 - 5.2 ადმინისტრაცია;
 - 5.3 პროფესიული განათლების მასწავლებელი;
 - 5.4 ტექნიკური პერსონალი.

თავი IV. გარდამავალი დებულებები

მუხლი 10. გარდამავალი დებულებები

1. სსიპ ილია წინამძღვრიშვილის სახელობის კოლეჯის საინფორმაციო ინფრასტრუქტურისა და IT პროცესების სისტემის ეფექტიანობისა და IT რისკების მართვის პოლიტიკა მტკიცდება და საჭიროებისამებრ ცვლილებების შეტანა ფორმდება კოლეჯის დირექტორის ინდივიდუალური ადმინისტრაციული სამართლებრივი აქტით.
2. წინამდებარე დოკუმენტში ცვლილებების შეტანის ინიცირება შეუძლია ინფორმაციული ტექნოლოგიების პოლიტიკის გატარებაზე პასუხისმგებელ პირს, რომელიც არგუმენტირებული მოთხოვნით მიმართავს კოლეჯის დირექტორს.
3. წინამდებარე დოკუმენტში ცვლილებების შეტანის შესახებ გადაწყვეტილებას იღებს დირექტორი.