

სსიპ კოლეჯი „ფაზისი“

საინფორმაციო ინფრასტრუქტურისა და IT
პროცესების სისტემის ეფექტიანობისა და IT
რისკების მართვის პოლიტიკა



2023 წელი

სარჩევი

თავი I. ზოგადი დებულებები.....	3
მუხლი 1. ზოგადი დებულებები	3
თავი II - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა	3
მუხლი 2. პასუხისმგებელი პირები.....	3
მუხლი 3. აპარატურის ფიზიკური უსაფრთხოება.....	3
მუხლი 4. ინფორმაციაზე წვდომის პოლიტიკა	4
მუხლი 5. პროგრამული უზრუნველყოფის პოლიტიკა.....	5
მუხლი 6. ქსელის მართვის პოლიტიკა.....	6
მუხლი 7. ინფორმაციული ტექნოლოგიების სისტემების განვითარების მექანიზმები.....	7
თავი III - ელექტრონული სისტემები.....	7
მუხლი 8. ელექტრონული საკომუნიკაციო სისტემები	7
მუხლი 9. ელექტრონული დოკუმენტბრუნვის სისტემა	8
მუხლი 10. ვებგვერდი	8
თავი IV. გარდამავალი დებულებები	9
მუხლი 10. გარდამავალი დებულებები	9

თავი I. ზოგადი დებულებები

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს სსიპ კოლეჯის „ფაზისი“ (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 ორივე ლოკაციაზე 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 ინფორმაციული ტექნოლოგიების სპეციალისტი.

მუხლი 3. აპარატურის ფიზიკური უსაფრთხოება

1. კოლეჯი ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის და/ან მგრძობელობის ინფორმაციას. აღნიშნული მოწყობილობები განთავსებულია დაცულ ადგილას.
2. 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.
3. კომპიუტერული ტექნიკის დაზიანების ან პროგრამული ხარვეზის შემთხვევაში, თითოეული თანამშრომელი ვალდებულია დაუყოვნებლივ აცნობოს პრობლემა დაწესებულების ინფორმაციული ტექნოლოგიების სპეციალისტს.

4. კომპიუტერული ტექნიკის დაზიანების ან პროგრამული ხარვეზის შემთხვევაში, პროფესიული სტუდენტი/მსმენელი ვალდებულია დაუყოვნებლივ აცნობოს პრობლემა პროფესიული განათლების მასწავლებელს ან კოლეჯის ადმინისტრაციას.
5. დაწესებულების საოფისე/სასწავლო აუდიტორიის კომპიუტერული ტექნიკის დაკარგვის შემთხვევაში შესაბამისი პასუხისმგებელი პირი ვალდებულია დაუყოვნებლივ აცნობოს დირექტორს ან მისი არყოფნის დროს შესაბამის პასუხისმგებელ პირებს.
6. 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.
7. დაწესებულების თანამშრომლები და პროფესიულ სტუდენტები/მსმენელები ვალდებული არიან არ დაზიანონ 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. პაროლებთან მიმართებაში კოლეჯის ყველა თანამშრომელი ვალდებულია:
 - 5.1 ნებისმიერი დროებითი პაროლი შეცვალოს გამოყენებისთანავე;
 - 5.2 პაროლში გამოიყენოს მინიმუმ 8 სიმბოლო (სასურველია დიდი ასოს, პატარა ასოს და რიცხვის კომბინაცია);
 - 5.3 არ ჩაიწეროს პაროლები ან არ გაამჟღავნოს სხვა პირებთან;
 - 5.4 ელექტრონული ფოსტით კომუნიკაციისას არ გაგზავნოს პაროლი ღია ტექსტის სახით;
 - 5.5 მომხმარებლები თვითონ არიან პასუხისმგებლები საკუთარი პაროლების უსაფრთხოებაზე და საიდუმლოებაზე.
6. პაროლების გაზიარება ჩაითვლება აღნიშნული პოლიტიკის დარღვევად და შესაძლოა გამოიწვიოს დისციპლინური პასუხისმგებლობის ზომების მიღება.
7. დაუყოვნებლივ უნდა მოხდეს იმ თანამშრომლის მომხმარებლების ანგარიშის დაბლოკვა, რომელმაც დატოვა სამსახური.
8. ნებისმიერი ინციდენტი, რომელიც ეხება კოლეჯის ინფორმაციული ტექნოლოგიების სისტემებზე არაავტორიზებულ წვდომას, დაუყოვნებლივ უნდა ეცნობოს ინფორმაციული ტექნოლოგიების სპეციალისტს.

9. 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. ინფორმაციული ტექნოლოგიების სპეციალისტთან 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 ინფორმაციული ტექნოლოგიების სპეციალისტი, რომელიც აკონტროლებს ქსელურ ნაკადს, რათა შეინარჩუნონ უსაფრთხოება და ქსელის მთლიანობა.
4. კოლეჯის შიდა ქსელი დაყოფილია ლოგიკურ ქვექსელებად (დომეინებად) - ადმინისტრაციისთვის და სასწავლო პროცესისთვის. დომეინებს შორის მოქმედებს მარშუტიზაცია და წვდომის კონტროლები.
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, ინფორმაციული ტექნოლოგიების სპეციალისტს, 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. ნებისმიერი ინციდენტი, რომელიც ეხება კოლეჯის ქსელს დაუყოვნებლივ უნდა ეცნობოს ინფორმაციული ტექნოლოგიების სპეციალისტს.
16. 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 Microsoft Teams-ის პლატფორმას.
2. Microsoft Teams-ის პლატფორმაზე ადმინისტრაციისთვის, პროფესიული განათლების მასწავლებლებისთვის და პროფესიული სტუდენტებისთვის კოლეჯი იყენებს შესაბამის ანგარიშებს (Account).
3. Microsoft Teams-ის პლატფორმის საშუალებით:
 - 3.1 პროფესიული განათლების მასწავლებლებს შეუძლიათ დაგეგმონ და ჩაატარონ ონლაინ ლექციები და შეხვედრები;
 - 3.2 ადმინისტრაცია მართავს ონლაინ შეხვედრებს;
 - 3.3 პროფესიულ სტუდენტებს/მსმენელებს აქვთ საშუალება დაუკავშირდნენ ერთმანეთს და კოლეჯის ადმინისტრაციის წარმომადგენლებს, შექმნან ჯგუფები და განიხილონ სასწავლო პროცესთან დაკავშირებული საკითხები.
4. ელექტრონული ფოსტით კომუნიკაციისთვის კოლეჯის ადმინისტრაცია იყენებს ღია საფოსტო სერვერების ანგარიშებს.
5. ონლაინ შეხვედრებისთვის, საჭიროების შემთხვევაში, კოლეჯი ასევე იყენებს სხვა უფასო პროგრამებს, როგორცაა Zoom, Google Meet და ა.შ.
6. პროფესიულ სტუდენტებს/მსმენელებს, პროფესიული განათლების მასწავლებლებსა და ადმინისტრაციის წარმომადგენლებს შორის კომუნიკაციისთვის, გარდა Microsoft Teams-სა კოლეჯი იყენებს სხვადასხვა პლატფორმებს: Gmail, Facebook, phazisi.edu.ge

მუხლი 9. ელექტრონული დოკუმენტბრუნვის სისტემა

1. კოლეჯი დოკუმენტბრუნვის 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.

მუხლი 10. ვებგვერდი

1. კოლეჯის მფლობელობაშია დომეინი <http://www.phazisi.edu.ge/>
2. დომეინისთვის ვებგვერდის გაშვება ხორციელდება Hosting-ის საშუალებით.
3. ვებგვერდი ასრულებს საკომუნიკაციო და საინფორმაციო ფუნქციას და ითვალისწინებს ინფორმაციის გონივრულ ვადაში მიღების ინტერესს.
4. ვებგვერდის ადმინისტრირებას ახდენს შესაბამისი კომპეტენციის მქონე პირი.

თავი IV. გარდამავალი დებულებები

მუხლი 10. გარდამავალი დებულებები

1. სსიპ კოლეჯის „ფაზისი“ 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 -ინფორმაციული ტექნოლოგიების სპეციალისტს, რომელიც არგუმენტირებული მოთხოვნით მიმართავს კოლეჯის დირექტორს.
3. წინამდებარე დოკუმენტში ცვლილებების შეტანის შესახებ გადაწყვეტილებას იღებს დირექტორი.