

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები

## შინაარსი

მუხლი 1. ზოგადი დებულებები.....	3
მუხლი 2. დოკუმენტის მიზნები.....	3
მუხლი 3. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანერგვაში მონაწილე მართვის ორგანოები და სტრუქტურული ერთეულები.....	3
მუხლი 4. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა და პროცედურების ძირითადი პრინციპები და წესები.....	4
მუხლი 5. საავტორო უფლებებისა და ინტელექტუალური საკუთრების უფლებების დაცვის ვალდებულება.....	5
მუხლი 6. პერსონალური მონაცემების დაცვის ვალდებულება.....	5
მუხლი 7. არაავტორიზებული მომხმარებლისგან ინფორმაციის დაცვა.....	6
მუხლი 8. საინფორმაციო-ტექნოლოგიური პროცესების მონიტორინგის განსაკუთრებული უფლებამოსილება.....	6
მუხლი 9. ინფორმაციის დაცვის ვალდებულება და საგამონაკლისო შემთხვევები .	7
მუხლი 10. ქსელის მონიტორინგი.....	7
მუხლი 11. საინფორმაციო-საკომუნიკაციო საშუალებებთან წვდომის შეზღუდვის უფლებამოსილება.....	7
მუხლი 12. საინფორმაციო-ტექნოლოგიური საშუალებების დაცვა.....	7
მუხლი 13. მონაცემების დაცვა.....	8
მუხლი 14. მონაცემების აღდგენის ვალდებულება.....	8
მუხლი 15. ინციდენტების პრევენცია და შედეგებზე რეაგირება.....	8
მუხლი 16. მომხმარებლის ანგარიშის შექმნა და გაუქმება.....	9
მუხლი 17. მომხმარებლის პირადი ანგარიშის პაროლის ფორმირების წესი.....	10
მუხლი 18. პირადი ანგარიშის პაროლის მართვასთან დაკავშირებული წესები.....	11
მუხლი 19. ელექტრონული ფოსტის შექმნა.....	11
მუხლი 20. ფილიალის ელექტრონული ფოსტით სარგებლობის წესები.....	12
მუხლი 21. კომპიუტერული ქსელების მართვა და მონიტორინგი.....	13
მუხლი 22. ინტერნეტ მისამართების მართვა.....	14
მუხლი 23. ქსელური მარშრუტიზატორის/როუტერის ინსტალაცია და მართვა...	14
მუხლი 24. უსადენო ქსელების მართვა.....	14
მუხლი 25. საინფორმაციო-ტექნოლოგიური საშუალებებისა და ქსელების მონიტორინგი.....	15

## მუხლი 1. ზოგადი დებულებები

წინამდებარე დოკუმენტი ადგენს ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას ვებსტერ უნივერსიტეტი, ინკ.-ის ფილიალი საქართველოში (შემდგომში - ფილიალი) და განსაზღვრავს ინფორმაციული ტექნოლოგიების მართვასთან დაკავშირებულ პროცედურებს.

## მუხლი 2. დოკუმენტის მიზნები

1. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა და პროცედურების მიზანია ფილიალის მართვის, სასწავლო და კვლევით საქმიანობაში ინფორმაციული ტექნოლოგიების ეფექტიანი და უსაფრთხო დანერგვა და ინფორმაციული ტექნოლოგიების სისტემების მუდმივი განვითარება.
2. ფილიალის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები მიზნად ისახავს აგრეთვე GDPR-თან (General Data Protection Regulation/ევროკავშირის მონაცემთა დაცვის რეგულაცია) შესაბამისობის უზრუნველყოფას.

## მუხლი 3. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანერგვაში მონაწილე მართვის ორგანოები და სტრუქტურული ერთეულები

1. ფილიალის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანერგვაში მონაწილეობს ფილიალის მართვის ყველა ორგანო და სტრუქტურული ერთეულები.
2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანერგვასა და შესაბამისი პროცედურების განხორციელებაზე პასუხისმგებელი ძირითადი სტრუქტურული ერთეულია საინფორმაციო ტექნოლოგიების მენეჯერი.

3. ფილიალი უფლებამოსილია ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანერგვა და შესაბამისი პროცედურების განხორციელება უზრუნველყოს საქართველოს კანონმდებლობის შესაბამისად გაფორმებული ხელშეკრულების საფუძველზე, მომსახურების მიღების შედეგად.

#### მუხლი 4. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა და პროცედურების ძირითადი პრინციპები და წესები

ფილიალის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები ეყრდნობა შემდეგ პრინციპებს და წესებს:

- ა) უზრუნველყოფილია ინფორმაციული ტექნოლოგიების სფეროში საქართველოში მოქმედი კანონმდებლობის მოთხოვნების დაცვა და შესაბამისობა;
- ბ) ფილიალის ყველა თანამშრომლისა და სტუდენტისთვის უზრუნველყოფილია ფილიალის საინფორმაციო და საკომუნიკაციო ტექნოლოგიებთან და საშუალებებთან თავისუფალი წვდომა შესაბამისი პერსონალური ანგარიშის გამოყენებით;
- გ) ფილიალის კამპუსის ტერიტორიაზე ყველას შეუძლია ფილიალის ინტერნეტ სერვისებით თავისუფალი სარგებლობა;
- დ) ფილიალის საინფორმაციო ტექნოლოგიებზე წვდომის მოცულობა განისაზღვრება შესაბამისი ხელშეკრულებით;
- ე) ფილიალის საინფორმაციო ანგარიშების მართვასა და სარგებლობაზე მონიტორინგის განხორციელების უფლებამოსილება აქვს მხოლოდ საინფორმაციო ტექნოლოგიების მენეჯერს;
- ვ) ფილიალის საკუთრებაში ან კანონიერ მფლობელობაში არსებული საინფორმაციო-საკომუნიკაციო ტექნიკური საშუალებები ფილიალის მართვის ორგანოების და სტრუქტურული ერთეულების თანამშრომლებს, აგრეთვე, საჭიროების შემთხვევაში, სტუდენტებს გადაეცემა დროებით მასთან გაფორმებული ხელშეკრულების მოქმედების ვადის განმავლობაში;

ზ) ფილიალის საინფორმაციო-საკომუნიკაციო ტექნიკურ საშუალებებს მომხმარებელი იყენებს მხოლოდ მასთან გაფორმებული ხელშეკრულებით განსაზღვრული ვალდებულებების შესრულების მიზნით;

თ) ფილიალის საინფორმაციო-საკომუნიკაციო ტექნიკურ საშუალებებით გამოყენებისას მომხმარებელი ვალდებულია დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები და სახელშეკრულებო პირობები.

## მუხლი 5. საავტორო უფლებებისა და ინტელექტუალური საკუთრების უფლებების დაცვის ვალდებულება

1. ფილიალი ვალდებულია დაიცვას აკადემიური და მოწვეული პერსონალის, მართვის ორგანოებისა და სტრუქტურული ერთეულების თანამშრომლების, სტუდენტების, აგრეთვე ფილიალის პარტნიორების, დაინტერესებული მხარეებისა და სხვა პირების საავტორო უფლებები და ინტელექტუალური საკუთრება.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული საავტორო და ინტელექტუალური საკუთრების დაცვას ფილიალი უზრუნველყოფს საქართველოს კანონმდებლობის, მათ შორის, „საავტორო და მომიჯნავე უფლებების შესახებ“ საქართველოს კანონის შესაბამისად.

## მუხლი 6. პერსონალური მონაცემების დაცვის ვალდებულება

1. ფილიალი ვალდებულია დაიცვას საინფორმაციო სისტემებში განთავსებული მომხმარებლების პერსონალური ინფორმაცია.

2. დაუშვებელია პერსონალური მონაცემები გახდეს სხვა პირისთვის ხელმისაწვდომი, გარდა იმ შემთხვევისა, როცა მას აქვს შესაბამისი პირის დადგენილი წესით გაცემული თანხმობა ან როდესაც პერსონალურ მონაცემებზე წვდომა დაშვებულია საქართველოს კანონმდებლობით, მათ შორის, საქართველოს

ზოგადი ადმინისტრაციული კოდექსით და „პერსონალურ მონაცემთა დაცვი შესახებ“ საქართველოს კანონის შესაბამისად.

3. პერსონალურ მონაცემად მიიჩნევა ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.

4. პერსონალური მონაცემების დამუშავებისას ფილიალი ხელმძღვანელობს საქართველოს კანონმდებლობით, მათ შორის, „პერსონალურ მონაცემთა დაცვი შესახებ“ საქართველოს კანონით.

#### მუხლი 7. არაავტორიზებული მომხმარებლისგან ინფორმაციის დაცვა

ფილიალის საინფორმაციო-საკომუნიკაციო საშუალებებსა და მათში განთავსებულ ინფორმაციაზე დაშვება არ შეიძლება ჰქონდეს არაავტორიზებულ მომხმარებელს.

#### მუხლი 8. საინფორმაციო-ტექნოლოგიური პროცესების მონიტორინგის განსაკუთრებული უფლებამოსილება

1. საინფორმაციო-ტექნოლოგიური პროცესების მონიტორინგის განსაკუთრებული უფლებამოსილება აქვს მხოლოდ ინფორმაციული ტექნოლოგიების მენეჯერს რექტორის ნებართვის საფუძველზე.

2. საინფორმაციო-ტექნოლოგიურ სისტემაში, მათ შორის, მართვის ელექტრონულ პროგრამებთან/რესურსებთან და მონაცემთა ბაზებთან დაკავშირებული სისტემური პარამეტრების ცვლილების უფლებამოსილება აქვს მხოლოდ ინფორმაციული ტექნოლოგიების მენეჯერს რექტორის თანხმობის საფუძველზე.

## მუხლი 9. ინფორმაციის დაცვის ვალდებულება და საგამონაკლისო შემთხვევები

1. დაუშვებელია ფილიალში დაცული რაიმე სახის კონფიდენციალური ინფორმაციის, მათ შორის, კომერციული საიდუმლოების გაცემა მესამე პირზე.
2. კონფიდენციალური ინფორმაციის გაცემა დასაშვებია მხოლოდ კანონმდებლობით დადგენილ შემთხვევებში და წესით.

## მუხლი 10. ქსელის მონიტორინგი

ვირუსების გავრცელების პრევენციის, პროგრამული პრობლემების აღმოფხვრის ან რაიმე სხვა სახის დამაზიანებელი აქტივობისაგან ფილიალის საინფორმაციო-საკომუნიკაციო სისტემების დაცვის მიზნით, დასაშვებია საინფორმაციო-საკომუნიკაციო ქსელის მონიტორინგი.

## მუხლი 11. საინფორმაციო-საკომუნიკაციო საშუალებებთან წვდომის შეზღუდვის უფლებამოსილება

ფილიალს აქვს უფლება წვდომა საინფორმაციო-საკომუნიკაციო საშუალებებთან წვდომა შეუზღუდოს მომხმარებელს, რომელიც არღვევს საინფორმაციო-საკომუნიკაციო საშუალებებით სარგებლობის წესებს ან სხვაგვარად ხელს უშლის საინფორმაციო-საკომუნიკაციო საშუალებებით დადგენილი წესით გამოყენების უფლებას.

## მუხლი 12. საინფორმაციო-ტექნოლოგიური საშუალებების დაცვა

1. ფილიალი განსაკუთრებულად იცავს არსებულ საინფორმაციო-ტექნოლოგიურ საშუალებებს, რისთვისაც იყენებს, მათ შორის, გარემოს უსაფრთხოებისა და მონიტორინგის მექანიზმებს.

2. ფილიალი უზრუნველყოფს საინფორმაციო-საკომუნიკაციო საშუალებების დაცვას კიბერ-თავდასხმებისა და ვირუსების გავრცელებისაგან შესაბამისი ანტი-ვირუსების ინსტალაციით და სხვა სათანადო ღონისძიებების გატარებით.

### მუხლი 13. მონაცემების დაცვა

1. ფილიალი უზრუნველყოფს მართვის პროცესში, აგრეთვე საგანმანათლებლო და სამეცნიერო საქმიანობის დროს მიღებული მონაცემების სათანადოდ შენახვას და ასლების შექმნას.

2. ფილიალი უზრუნველყოფს მომხმარებელთა მხარდაჭერას, მათ შორის, იმ შემთხვევაშიც, როცა მომხმარებლის პირად საინფორმაციო-საკომუნიკაციო საშუალებების ფუნქციონირებას შეექმნება ინფორმაციისა და მონაცემების დაკარგვის საფრთხე.

3. ამ მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევაში, ფილიალი არ არის პასუხისმგებელი ინფორმაციისა და მონაცემების დაკარგვაზე, თუ ეს გამოწვეულია მომხმარებლის მიერ პირადი საინფორმაციო-ტექნოლოგიური საშუალებით ინფორმაციისა და მონაცემების შესაბამისი დაცვის გარეშე და დადგენილი წესების დარღვევით გამოყენებით.

### მუხლი 14. მონაცემების აღდგენის ვალდებულება

ფილიალი უზრუნველყოფს ინფორმაციისა და მონაცემების დაცვას და აღდგენას, მათ შორის, ელექტროენერჯის გათიშვის ან სხვაგვარი ფორს-მაჟორული სიტუაციების შემთხვევაში.

### მუხლი 15. ინციდენტების პრევენცია და შედეგებზე რეაგირება



1. ფილიალი საინფორმაციო-საკომუნიკაციო სისტემების დაცვის მიზნით, უზრუნველყოფს ინფორმაციულ უსაფრთხოებას, რისთვისაც:

ა) ახდენს რისკების იდენტიფიცირებას;

ბ) შეისწავლის ცალკეულ შემთხვევას;

გ) აღწერს და აფასებს რისკებსა და მატერიალიზებულ შემთხვევებს;

დ) შეიმუშავებს რეაგირების ღონისძიებებს.

2. იმ შემთხვევაში, თუ რისკის პრევენცია არ არის შესაძლებელი და ინციდენტი მატერიალიზებულია, ფილიალი უზრუნველყოფს ინციდენტის შესახებ ინფორმაციის დაუყოვნებლივ გადაცემას სხვა, დაუზიანებელი ინფორმაციისა და მონაცემების დაცვის მიზნით.

3. რისკების იდენტიფიცირების ან/და მატერიალიზებული ინციდენტის შემთხვევაში, ინფორმაციული ტექნოლოგიების მენეჯერი ადგენს ანგარიშს, რომელსაც განსახილველად წარუდგენს რექტორს.

#### მუხლი 16. მომხმარებლის ანგარიშის შექმნა და გაუქმება

1. ფილიალის მართვის ორგანოს ყველა წევრს, სტრუქტურული ერთეულის თითოეულ თანამშრომელს, აკადემიურ და მოწვეულ პერსონალს, აგრეთვე, სხვა პირს, თუ ის თანამშრომლობს ფილიალთან რაიმე სხვა ფორმით, აქვს პირადი ანგარიში საინფორმაციო-ტექნოლოგიური რესურსებისა და ელექტრონული ფოსტის გამოყენების მიზნით.

2. ფილიალის საბაკალავრო და სამაგისტრო საგანმანათლებლო პროგრამების ყველა სტუდენტს აქვს პირადი ანგარიში საინფორმაციო-ტექნოლოგიური რესურსებისა და ელექტრონული ფოსტის გამოყენების მიზნით.

3. ამ მუხლის პირველ პუნქტში მითითებული პირებისთვის პირადი ანგარიში იქმნება შესაბამისი ხელშეკრულების გაფორმებისთანავე, ხოლო ამ მუხლის მე-2 პუნქტში მითითებული პირებისთვის - სტუდენტის სტატუსის წარმოშობისთანავე.

4. ამ მუხლის პირველი და მე-2 პუნქტებით გათვალისწინებული პირებისთვის ანგარიშების შექმნას უზრუნველყოფს ფილიალის ინფორმაციული ტექნოლოგიების მენეჯერი.
5. ინფორმაციული ტექნოლოგიების მენეჯერს ფილიალის თანამშრომლებისთვის პირადი ანგარიშების შექმნის შესახებ ინფორმაციას აწვდის ფილიალის ადამიანური რესურსების მართვის მენეჯერი, ხოლო სტუდენტების შესახებ ინფორმაციას - სტუდენტთა მიღების კონსულტანტი.
6. ფილიალის თანამშრომლის პირადი ანგარიში უქმდება მასთან შესაბამისი ხელშეკრულების შეწყვეტის შემთხვევაში.
7. სტუდენტის მიერ საგანმანათლებლო პროგრამის დასრულების შემთხვევაში, ხდება მისი პირადი ანგარიშის შენარჩუნება და მისი ელექტრონული ფოსტა აისახება ფილიალის კურსდამთავრებულთა ბაზაში.
8. სტუდენტის სტატუსის შეჩერება არ იწვევს სტუდენტის პირადი ანგარიშის გაუქმებას. სტატუსის შეჩერების შემთხვევაში, სტუდენტს უნარჩუნდება საინფორმაციო-ტექნოლოგიურ რესურსებზე შეზღუდული წვდომა.

#### მუხლი 17. მომხმარებლის პირადი ანგარიშის პაროლის ფორმირების წესი

1. მომხმარებლის პირადი ანგარიშის პაროლი იქმნება მომხმარებლის ნამდვილობის შემოწმების მიზნით და უზრუნველყოფს მომხმარებლის პერსონალური და საინფორმაციო-ტექნოლოგიურ სისტემაში განთავსებული ინფორმაციის დაცვას.
2. პაროლის შედგენისას დაცულ უნდა იქნეს შემდეგი წესი:
  - ა) პაროლი უნდა შეიცავდეს ლათინური ანბანის როგორც დიდ, ისე პატარა სიმბოლოებს;
  - ბ) პაროლი უნდა შეიცავდეს ციფრს ან სხვა სიმბოლოებს (მაგალითად, 92%&-:\_)
  - გ) სიმბოლოთა რაოდენობა უნდა იყოს არანაკლებ რვისა;
  - დ) დაუშვებელია ისეთი მითითებების გამოყენება, როგორცაა, სახელი, გვარი, დაბადების თარიღი, ტელეფონის ნომერი და ა.შ.

3. ამ მუხლის მე-2 პუნქტით გათვალისწინებული პაროლის ფორმირებამდე, მომხმარებელი პირადი ანგარიშის შექმნისთანავე იღებს ერთჯერად პაროლს, რომელსაც ცვლის მომხმარებელი პირველივე გამოყენებისთანავე.

#### მუხლი 18. პირადი ანგარიშის პაროლის მართვასთან დაკავშირებული წესები

1. ფილიალის პირადი ანგარიშის მომხმარებელს პაროლის მართვასთან დაკავშირებით ეკისრება შემდეგი ვალდებულებები:

ა) დაუშვებელია ერთი და იგივე პაროლის გამოყენება ფილიალის ანგარიშებისა და სხვა, პირადი ანგარიშებისათვის;

ბ) დაუშვებელია პირადი ანგარიშის პაროლის სხვა პირისთვის გაზიარება;

გ) დაუშვებელია პაროლის გაგზავნა ელექტრონული ფოსტით ან სხვა საკომუნიკაციო საშუალებებით;

დ) რეკომენდირებულია მომხმარებელმა ბრაუზერში არ დაიმახოვროს პაროლი;

ე) პირადი ანგარიშით სარგებლობისას შეასრულოს პაროლის დაცვის სხვა გონივრული მოთხოვნები და, სათანადო რეკომენდაციის შემთხვევაში, შეცვალოს/განაახლოს პაროლი.

2. თუ არსებობს ეჭვი, რომ შესაძლოა პაროლი გამჟღავნდა ან/და ჩნდება პაროლის გამჟღავნების რისკი, მაშინ მომხმარებელი ვალდებულია დაუყოვნებლივ შეცვალოს პირადი ანგარიშის პაროლი.

#### მუხლი 19. ელექტრონული ფოსტის შექმნა

1. ფილიალში ელექტრონული ფოსტა იქმნება ფილიალის ყველა თანამშრომლისა და სტუდენტისათვის.

2. ელექტრონული ფოსტის მისამართის იქმნება მომხმარებლის სახელისა და გვარის მიხედვით.

3. თუ მომხმარებლის სახელის და გვარის მიხედვით უკვე შექმნილია ელექტრონული ფოსტა, მაშინ რეგისტრაციის თანმიმდევრობის მიხედვით ემატება რიგითი ნომერი.

4. ელექტრონული ფოსტა იქმნება ინფორმაციული ტექნოლოგიების მენეჯერის მიერ, რომელსაც თანამშრომლების შესახებ ინფორმაციას აწვდის ადამიანური რესურსების მენეჯერი, ხოლო სტუდენტების შესახებ ინფორმაციას - სტუდენტთა მიღების კონსულტანტი.

## მუხლი 20. ფილიალის ელექტრონული ფოსტით სარგებლობის წესები

1. ფილიალის თანამშრომლებს და სტუდენტებს აქვთ ელექტრონული ფოსტა @webster.edu, რომელიც გამოიყენება ფილიალის თანამშრომლებს, აკადემიურ და მოწვეულ პერსონალსა და სტუდენტებს შორის ოფიციალური კომუნიკაციის მიზნით.

2. დაუშვებელია მომხმარებლის მიერ ელექტრონული ფოსტით გაგზავნილი და მიღებული ინფორმაციისა და მიმოწერის მონიტორინგი.

3. მომხმარებელი ელექტრონული ფოსტით სარგებლობისას ითვალისწინებს შემდეგ წესებს:

ა) აკრძალულია კომერციული საქმიანობის შესახებ ინფორმაციის გავრცელება ამ საქმიანობის რეკლამირების მიზნით;

ბ) აკრძალულია პოლიტიკური საქმიანობის შესახებ ან პოლიტიკური აქტივობისადმი მხარდაჭერის ან პოლიტიკურ საქმიანობასთან დაკავშირებით რაიმე სხვა სახის ინფორმაციის გავრცელება;

გ) უხამსობის ან მცდარი ინფორმაციის გავრცელება, სხვა პირის ცილისწამება, ყალბი ინფორმაციის მიწოდება, თაღლითობა, დაშინება, სხვა პირზე ზეწოლა ან ელექტრონული ფოსტის მეშვეობით რაიმე სხვა უკანონო ქმედების ჩადენა;

დ) დაუშვებელია ელექტრონული ფოსტის გამოყენებით სხვა პირის შეურაცხყოფა.

4. ელექტრონული ფოსტის ანგარიშით სარგებლობა შეჩერდება:

- ა) ფილიალის თანამშრომელთან შრომითი ხელშეკრულების შეწყვეტისას;
  - ბ) სტუდენტის სტატუსის შეწყვეტის ან მობილობის წესით გადასვლის შემთხვევაში;
  - გ) ელექტრონული ფოსტის კანონმდებლობის საწინააღმდეგოდ, ამ წესის ან ფილიალში მოქმედი შიდა სამართლებრივი აქტების საწინააღმდეგოდ გამოყენების შემთხვევაში, აგრეთვე, ამ ქვეპუნქტით გათვალისწინებული ფაქტის დადგენის მიზნით დაწყებული წარმოების დასრულებამდე;
  - დ) აკრძალული ინფორმაციის გავრცელების შემთხვევაში;
  - ე) სხვა პირის მიერ მომხმარებლის ელექტრონულ ფოსტაზე წვდომის მოპოვების შემთხვევაში.
5. ელექტრონული ფოსტით სარგებლობა მომხმარებელს შესაძლოა შეეზღუდოს ფილიალის საინფორმაციო-ტექნოლოგიურ სისტემაში ტექნიკური პრობლემის წარმოქმნის შემთხვევაშიც, რის შესახებაც ინფორმაციული ტექნოლოგიების მენეჯერი დაუყოვნებლივ ატყობინებს მომხმარებელს.
6. აკრძალულია ელექტრონული ფოსტის ანგარიშის წაშლა, მათ შორის, იმ შემთხვევაშიც, თუ ფილიალის თანამშრომელთან შეწყდება სახელშეკრულებო ურთიერთობა ან სტუდენტს შეუწყდება სტატუსი.

## მუხლი 21. კომპიუტერული ქსელების მართვა და მონიტორინგი

1. ფილიალის სადენიანი და უსადენო ქსელების, მონაცემთა გადაცემის ინფრასტრუქტურას და მონაცემთა ბაზების და სხვა სახის სერვერების შეუფერხებელ და გამართულ ფუნქციონირებას უზრუნველყოფს ინფორმაციული ტექნოლოგიების მენეჯერი.
2. ყველა სახის ტექნიკური სამუშაო ან პროგრამული განახლება, რომელიც იწვევს ქსელის ფუნქციონირებაში შეფერხებას, ხორციელდება არასამუშაო საათებში, ხოლო ქსელის ფუნქციონირების შეფერხების შესახებ ინფორმაცია მომხმარებლებს მიეწოდებათ სულ მცირე ერთი დღით ადრე.

## მუხლი 22. ინტერნეტ მისამართების მართვა

1. საინფორმაციო-საკომუნიკაციო საშუალებების ინტერნეტ მისამართების განაწილება ხდება სერვერის გამოყენებით და უზრუნველყოფილია მისი გამართული ფუნქციონირება და ადმინისტრირება.
2. ქსელში ჩართულ საინფორმაციო-საკომუნიკაციო საშუალებებს ენიჭება დინამიური (დროებითი) ან სტატიკური (მუდმივი) ინტერნეტ მისამართი.
3. სტატიკური (მუდმივი) ინტერნეტ მისამართის მინიჭება ხდება უსაფრთხოების მიზნით და გამონაკლის შემთხვევებში.

## მუხლი 23. ქსელური მარშრუტიზატორის/როუტერის ინსტალაცია და მართვა

1. ფილიალში ყველა მარშრუტიზატორის/როუტერის ქსელში ჩართვა, მონტაჟი და ინსტალაცია ხორციელდება უსაფრთხოების წესების დაცვით, რასაც უზრუნველყოფს ინფორმაციული ტექნოლოგიების მენეჯერი.
2. მარშრუტიზატორის/როუტერის გამოყენების დროს უზრუნველყოფილია წვდომის პაროლის დაშიფრული ფორმით შენახვა, SNMP სათანადო პროტოკოლის გამოყენება მართვისა და მონიტორინგისთვის, ხოლო მარშრუტიზაციის დაშორებული კონფიგურაციისთვის გამოიყენება დაშიფრული არხი (ssh).
3. ქსელური მარშრუტიზაციის მონიტორინგი მიმდინარეობს ოცდაოთხსაათიან რეჟიმში, ყოველ დღე, ხოლო წლის განმავლობაში არანაკლებ ორჯერ ტარდება ქსელური მარშრუტიზაციის სრული მონიტორინგი.
4. ამ მუხლის მე-3 პუნქტით გათვალისწინებული მონიტორინგის ანგარიშის შედეგები წარედგინება რექტორს.

## მუხლი 24. უსადენო ქსელების მართვა

1. ფილიალში უსადენო ქსელებში დაშვება შესაძლოა იყოს შეზღუდული ან თავისუფალი.
2. შეზღუდული წვდომის ქსელის შემთხვევაში, ქსელზე წვდომის პაროლი აქვს მხოლოდ უფლებამოსილ პირებს, რომელთაც პაროლს აცნობს ინფორმაციული ტექნოლოგიების მენეჯერი.
3. თავისუფალი დაშვების შემთხვევაში, ქსელზე წვდომა აქვს კამპუსში მყოფ ნებისმიერ პირს, რომელსაც თავისუფალ ქსელზე დაშვების პაროლი გადაეცემა პირადად, კამპუსის ტერიტორიაზე საჯაროდ გამოქვეყნების ან სხვაგვარი ფორმით.
4. უსადენო ქსელთან დაშვება ხდება WPA2/PSK სპეციფიკაციებითა და AES სტანდარტით.

#### მუხლი 25. საინფორმაციო-ტექნოლოგიური საშუალებებისა და ქსელების მონიტორინგი

1. ფილიალის ქსელში ჩართული ყველა საინფორმაციო-ტექნოლოგიური საშუალება ფუნქციონირებს ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა და პროცედურების მიხედვით.
2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა და პროცედურების ნებისმიერი ფორმით დარღვევის ან დარღვევის რისკის შემთხვევაში ფილიალი უფლებამოსილია განახორციელოს კონკრეტული საინფორმაციო-ტექნიკური საშუალებების მონიტორინგი შინაარსობრივი კონტროლის გარეშე.
3. ამ მუხლის მე-2 პუნქტით განსაზღვრულ ფუნქციას ასრულებს მხოლოდ ინფორმაციული ტექნოლოგიების მენეჯერი, რომელიც მონიტორინგის შედეგების შესახებ ინფორმაციას აწვდის რექტორს.