EEU

ინფორმაციული ტექნოლოგიების და პროგრამულ პლატფორმებისა და სისტემების მართვისა პოლიტიკა

დამტკიცებულია: *უნივერსიტეტის რექტორის 2019 წლის 7 თებერვლის №08/01-08 ბრძანებით*
განახლებულია: *წარმომადგენლობითი საბჭოს 2020 წლის 25 აგვისტოს №05დადგენილებით*

1. დოკუმენტის მიზნები

ინფორმაციული ტექნოლოგიებისა და პროგრამულ პლატფორმებისა და სისტემების მართვისა პოლიტიკის დოკუმენტის მიზანს წარმოადგენს განსაზღვროს აღმოსავლეთ ევროპის უნივერსიტეტის (შემდგომში - უნივერსიტეტი) განსაზღვროს უნივერსიტეტის საქმიანობაში ინფორმაციული ტექნოლოგიის მართვისა და ინფორმაციული უსაფრთხოებასთან დაკავშირებული პოლიტიკა და პროცედურები, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმები, მომხმარებელთა უფლება-მოვალეობები.

2. დოკუმენტის გამოყენების სფერო

ინფორმაციული ტექნოლოგიებისა და პროგრამულ პლატფორმებისა და სისტემების მართვისა პოლიტიკის (შემდგომში - „პოლიტიკა“) სავალდებულოა გამოსაყენებლად ყველა იმ პირის მიერ, რომელიც გაჩნია ლეგიტიმური უფლება და თავის ადმინისტრაციულ, აკადემიურ თუ სწავლა/სწავლების საქმიანობაში იყენებს უნივერსიტეტის ინფორმაციულ ტექნოლოგიებსა და რესურსებს. აგრეთვე სათანადო წესით მოწვეულ ყველა პიროვნებისათვის, რომელიც ენიჭება უფლება იქონიოს წვდომა უნივერსიტეტის კომპიუტერული რესურსებზე.

3. მარეგულირებელი დოკუმენტები

ინფორმაციული ტექნოლოგიებისა და პროგრამულ პლატფორმებისა და სისტემების მართვისა პოლიტიკა ეყრდნობა საქართველოში მოქმედ კანონმდებლობას, საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სფეროსი სტანდარტებს, ინტელექტუალური საკუთრებისა და პერსონალური მონაცემთა დაცვის საკითხებში შესაბამის კანონმდებლობის აქტებსა და უნივერსიტეტის შინაგანაწეს.

ინფორმაციული ტექნოლოგიებისა და პროგრამულ პლატფორმებისა და სისტემების მართვისა პოლიტიკა

1. პოლიტიკის გამოყენების ზოგადი მოთხოვნები

აღმოსავლეთ ევროპის უნივერისტეტი დეკლარირებული მისიის განსახორციელებლად საკუთარი საქმიანობისას საგანმანათლებლო და მმართველობით პროცესებში ფართოდ იყენებს საინფორმაციო-საკომუნიკაციო ტექნოლოგიებს, პროგრამულ პლატფორმებსა და სისტემებს, რომელთა ეფექტიან და უსაფრთხო ფუნქციონირებას უზრუნველყოფს თანამდროვე და მაღალტექნოლოგიური ინფრასტრუქტურის გამოყენებით. მათ შორის:

- უნივერსიტეტის ნებისმიერი სტუდენტისათვის და პერსონალისათვის ინტერნეტთან და უნივერსიტეტის შიდა რესურსებთან (პროგრამულ პლატფორმებთან და სისტემებთან, კორპორატიულ ფოსტასთან) შეუფერხებელი და დაცული წვდომა უნდა იყოს უზრუნველყოფილი, როგორც სადენიანი, ასევე უსადენო ტექნოლოგიების გამოყენებით;
- მონაცემთა დაცულობაზე და ეფექტიანი მართვისთვის გამოყენებული უნდა იქნეს დაცულ მონაცემთა და აპლიკაციების სერვერები, რომლებიც განთავსება შესაძლებელია როგორც უნივერსიტეტის ტერიტორიაზე სპეციალურად მოწყობილ ფართში, ასევე ხელშეკრულების საფუძველზე კონტრაქტორ კომპანიასთან, დაცული ღრუბლოვანი (Cloud) ტექნოლოგიების გამოყენებით;
- პროგრამულ პლატფორმები და სისტემების განვითარება წარმოადგენს უნივერსიტეტის პრიორიტეტულ მიმართულებას, ისინი მაქსიმალურად უნდა იქნეს გამოყენებული უნივერსიტეტის საგანმანათლებლო და მმართველობით პროცესებში, რომელებიც

საჭიროებს მონაცემების მოქნილ მართვას, დაცულობას და პერსონალურ ინფორმაციასთან წვდომის შეზღუდვას, პროგრამულ პლატფორმები და სისტემების გამოყენება სავალდებულოა სასწავლო პროცესების, პერსონალისა და ფინანსების მართვაში;

- საინფორმაციო-საკომუნიკაციო სიტემაში ნებისმერი პროგრამულ თუ აპარატულ რესურსთან წვდომა უნდა ხდებოდეს პაროლური სისტემისა და ინფორმაციული უსაფრთხოების სფეროს სანდო, სტანდარტების, მეთოდებისა და პროტოკოლების გამოყენებით.

2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის მიზანია ხელი შეუწყოს უნივერსიტეტში ინფორმაციის ძირითადი მახასიათებლების დაცვას (კონფიდენციალურობა, ხელმისაწვდომობა, მთლიანობა), რაც თავის მხრივ უზრუნველყოფს ინფორმაციული რისკების მართვის ეფექტიანობას და ბიზნესუწყვეტობას.

იგი განსაზღვრავს უნივერსიტეტის მმართველობით, საგანმანათლებლო და კვლევით პროცესებში კომპიუტერული და საინფორმაციო რესურსების გამოყენების საკითხში ზოგად მიდგომებს და წესებს, რომლის საფუძველზეც მოხდება ინფორმაციული ტექნოლოგიის მართვის პროცედურების ფორმირება.

უნივერსიტეტში ინფო*რმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:*

- უნივერსიტეტის ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა;
- უნივერსიტეტში არსებული ძირითადი მონაცემები და ინფორმაცია;
- პირები, რომლებიც იყენებენ ან/და ახორციელებენ ინფორმაციული

  სისტემების ადმინისტრირებას;

პოლიტიკის გატარების შედეგად უნდა უზრუნველყოფილი იქნეს:

1.1. **ფიზიკური უსაფრთხოება** - უნდა ხორციელდებოდეს კონტროლი ინფორმაციულ აქტივებზე არაავტორიზებულ წვდომის, ჩარევის, დატაცებისა ან დაზიანების თავიდან ასაცილებლად. სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ფიზიკური, ტექნიკური, პროცედურული და გარემოს უსაფრთხოების კონტროლის მექანიზმებით. უნივერსიტეტი ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის და/ან მგრძნობელობის ინფორმაციას. ასეთი მოწყობილობები განთავსებულია ფიზიკურად დაცულ ადგილას.

1.2. **ინფორმაციული უსაფრთხოების ინციდენტების მართვა** - უნდა უზრუნველყოფილი იქნეს უსაფრთხოების ინციდენტების იდენტიფიცირება, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, მათი წყაროების (შიდა, გარე) და ფორმების (DDoS, Keylog და სხვა) დადგენას და ადეკვატურ რეაგირებას, ასევე საჭიროების შემთხვევაში რეკომენდაციების შემუშავებას.

1.3. **კომუნიკაციებისა და ოპერაციების მართვა** - მუდმივ უნდა ხორციელდებოდეს კონტროლს ინფორმაციის დამამუშავებელ მოწყობილობებზე მათი სწორი და უსაფრთხო სარგებლობის უზრუნველყოფის მიზნით. ქსელის მონიტორინგი ხორციელდება 24-საათიან რეჟიმში. პროცესების მიმდინარეობის ეტაპობრივი სტრუქტურა შემდეგნაირია:

- შეტყობინება დაზიანების შესახებ;
- ოპერატორი მართვის პანელიდან ახდენს დაზიანების იდენტიფიცირება და აღმოფხვრას;
- ოპერატორის საჭიროების შემთხვევაში მიდის დაზიანების ადგილას
- თუ დაზიანების აღმოფხვრა ვერ მოხერხდა, ატყობინებს ადმინისტრატორს
- ადმინისტრატორი ატარებს ქსელის დიაგნოსტიკას
- ოპერატორი ატყობინებს მომხმარებელს დაზიანებისა და გამოსწორების სავარაუდო ვადებს;

1.4. **საზიანო პროგრამებზე კონტროლი** - მუდმივად უნდა ხორციელდებოდეს სისტემის კონტროლი და დაცვის სისტემის მუდმივი განახლება, რათა თავიდან აცილებული იქნეს კრიტიკულ სისტემებში როგორც საზიანო ან თაღლითური პროგრამების გამოყენება ასევე ვირუსების გავრცელება უნივერსიტეტის შიგნით და უნივერსიტეტის მიზეზით – მის გარეთ;

1.5. **სისტემების, აპლიკაციების და მონაცემთა რეზერვირება** - სისტემატიურად უნდა ხორციელდებოდეს ყველა კრიტიკული სისტემის, აპლიკაციის და მონაცემების სარეზერვო ასლების შენახვა და განვითარებას;

1.6. **კომპიუტერული ქსელის მართვა** - მუდმივად უნდა ხორციელდებოდეს როგორც სადენიანი ასევე უსადენო ქსელების სისტემის კონტროლი როგორც ფიზიკურ ასევე ქსელურ დონეზე რათა დროულად იქნეს გამოვლენილი და აღმოფხვრილი სისტემაში უცხო, არაავტორიზებულ მომხმარებლის შეჭრის ფაქტი.

1.7. **ახალი სისტემის დაგეგმვა-შემუშავება** - სისტემების დაგეგმვისა და დანერგვის პროცესში გათვალისწინებულ უნდა იქნეს არსებული სისტემების ტექნიკური და ფუნქციური შესაძლებლობები, რათა არ მოხდეს კრიტიკული სისტემების გამართული მუშაობის შეფერხება.. რისთვისაც სისტემების ტესტირება ხდება იზოლირებულ გარემოში, რათა სასიცოცხლოდ მნიშვნელოვანი კრიტიკული სისტემები დაცულ იქნეს შეცდომით განადგურების და/ან დაზიანებისაგან.

3. მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა

მომხმარებლის უფლება წარმოადგენს კომპიუტერულ რესურსებთან წვდომის წესების ერთობლიობას, რომელიც განსაზღვრავს მონაცემებზე ჩასატარებელი მოქმედებებს: წაკითხვა, ჩაწერა, შესრულება, ცვლილება, ადმინისტრირება.

მომხმარებელს მხოლოდ იმ კონკრეტულ რესურსებთან მიწვდომის უფლება ენიჭება, რომლებიც საჭიროა მისი უშუალო სამსახურეობრივი/აკადემიური მოვალეობების შესასრულებლად. უფლებები განისაზღვრება (იცვლება ან/და უქმდება) მისი დეპარტამენტის (სამსახურის) ხელმძღვანელის მიერ. მომხმარებლებს ეკრძალებათ საერთო მოხმარების რესურსების გარდა სხვა კომპიუტერული რესურსის გამოყენება ავტორიზაციის გარეშე.

თუ მომხმარებელი შეიცვლის თანამდებობას ან/და პასუხისმგებლობას უნივერსიტეტში, მომხმარებლის წვდომის უფლებები უნდა გადაიხედოს. მომხმარებელმა უნდა გამოიყენოს კომპიუტერული რესურსების მხოლოდ ის ობიექტები, ანგარიშები, წვდომის კოდები, პრივილეგიები ან/და ინფორმაცია, რომლისთვისაც არის უფლებამოსილი მისი ახალი თანამდებობის პასუხისმგებლობის მიხედვით.

4. მომხმარებელთა უფლება-მოვალეობები

საუნივერსიტეტო საზოგადოების ყველა წევრსა და ჯგუფს, გააჩნიათ შესაძლებლობა რათა ყოველთვე შეზღუდვების გარშე ჰქონდეთ წვდომა უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემებთან.

უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემებისა ან რესურსების გამოყენება დასაშვებია მხოლოდ ავტორიზებული მომხმარებლისათვის, რისთვისაც იგი ვალდებულია გამოიყენოს თავისი პერსონალური ანგარიში, დადგენილი წესით და ხელშეკრულების განსაზღვრული უფლებამოსილების ფარგლებში. პერსონალური ანგარიშების ადმინისტრირებასა და გამოყენების მონიტორინგს ახორციელებს ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი.

უნივერსიტეტის მფლობელობაში ან ზედამხედველობის ქვეშ მყოფი საინფორმაციო-საკომუნიკაციო ტექნიკა მომხმარებელს დროებით სარგებლობაში გადაეცემა სამუშაო ანდა სასწავლო ხელშეკრულების მოქმედების პერიოდში (შემდგომში - ხელშეკრულება). მომხმარებელი ვალდებულია გამოიყენოს უნივერსიტეტის არსებული საინფორმაციო-საკომუნიკაციო ტექნიკა ან/და პროგრამული უზრუნველყოფა მხოლოდ კანონიერი მიზნებით, რომლებიც არ ეწინააღმდეგებიან საქართველოს კანონმდებლობასა და უნივერსიტეტის წესდებას. აგრეთვე დაუშვებელია გამოყენებულ იქნეს რომელიმე პიროვნების ცილისწამებისა და შეურაცხყოფის მიზნით.

უნივერსიტეტი უზრუნველყოფს როგორც მისი სტუდენტების, აკადემიური და სამეცნიერო პერსონალის მიერ ასევე სხვა ფიზიკური და იურიდიული პირების მიერ შემუშავებული და მისი საინფორმაციო-საკომუნიკაციო სისტემებში განთავსებულ პროგრამული უზრუნველყოფის, მონაცემთა ბაზების და სხვა ელექტრონული ფორმატით წარმოდგენილი ნამუშევრების (ლიტერატურული, მუსიკალური თუ მხატვრული ნაწარმოებების, ფოტოსურათების, კინოფილმების, ვიდეოჩანაწერების და სხვა), საავტორო უფლებებისა და ინტელექტუალური საკუთრების უფლების დაცვას და შესაბამის პროცედურებით უზრუნველყოფს საავტორო უფლებების დარღვევების პრევენციას.

5. ინფორმაციული უსაფრთხოება

უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემები იმგვარად უნდა იყოს მოწყობილი, რათა უზრუნველყოს სამეწარმეო, სამუშაო, პერსონალური, პირადი ინფორმაციისა და მონაცემების დაცულობა და მთლიანობა, რისთვისაც ნებისმიერ მომხმარებელს[1]

- ☐ არ შეეძლოს მესაკუთრის თანხმობის გარეშე: დაათვალიეროს, შექმნას ასლი, შეცვალოს ან წაშალოს ელექტრონული ფაილები და მონაცემთა ბაზებში ინფორმაცია,
- ☐ მოახდინოს სისტემური პარამეტრების ცვლილება
- ☐ სათანადო ნებართვის გარეშე მიიღოს წვდომა საუნივერსიტეტოს მართვის, სწავლებისა და სამეცნიერო მონაცემთა ბაზებთან, პროგრამებთან და აპლიკაციებთან.
- ☐ სათანადო ნებართვის გარეშე მესამე პირებს არ გადასცენ უნივერსიტეტის საინფორმაციო-საკომუნიკაციო რესურსებზე დაცული ინფორმაცია, თავისი ანდა სხვისი მომხმარებლის ანგარიშის პარამეტრები და პერსონალური მონაცემების შემცველი ინფორმაცია, აგრეთვე მონაცემები, რომელიც წარმოადგენს უნივერსიტეტისათვის საკუთრებას და არის კონფიდენციალური, კომერციული საიდუმლოება ან/და დაცულია საავტორო უფლებით.

[1] საინფორმაციო-საკომუნიკაციო სისტემის ადმინისტრატორის გარდა, მოქმედი კანონმდებლობის გათვალისწინებით

უნივერსიტეტი ჩვეულებრივ არ ახდენს მომხმარებლების მიერ კომპიუტერულ ქსელში გადაცემული მასალის შემოწმებასა ანდა რაიმე ფორმით შეზღუდვას. თუმცა განსაკუთრებულ შემთხვევებში (სისტემური პრობლემების აღმოსაფხვრელად, ვირუსებისა და სხვა საზიანო პროგრამების მონიტორინგისა და აღმოფხვრის მიზნითა და კანონით განსაზღვრულ სხვა შემთხვევებში) უნივერისტეტი იტოვებს უფლებას ღიად მოახდინოს მომხმარებლის საინფორმაციო რესურსების გამოყენებისა და სამუშაო სესიების მონიტორინგი, რომლის შესახებ ეცნობება მას.

უნივერსიტეტი, კომპიუტერული რესურსების გამოყენების წესების დარღვევის შემთხვევაში იტოვებს უფლებას შეუზღუდოს დამრღვევ მომხმარებელს უნივერსიტეტის საინფორმაციო რესურსებთან მიწვდომის უფლება. განსაკუთრებით მძიმე დარღვევის შემთხვევაში მომხმარებლის პირადი კომპიუტერი შესაბამის შეტყობინების გაგზავნის შემდეგ დაუყონებლივ გაითიშება უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემებთან.

6. მონაცემთა დაცვა

ინფორმაციული უსაფრთხოების მიხედვით მონაცემთა კლასიფიკაცია ხორციელდება რისკების, მისი კონფიდენციალობის, ღირებულებისა და უნივერსიტეტის საქმიანობაზე გავლენის დონის მიხედვით. უნივერსიტეტის ყველა მონაცემი უნდა იყოს კლასიფიცირებული შემდეგი სამი ტიპის მიხედვით:

- **შეზღუდული** - მონაცემთა არასანქცირებული გამჟღავნება დაკავშირებულია მაღალ რეპუტაციული და ორგანიზაციულ რისკებთან და მათი შეცვლამ ან განადგურებამ შეიძლება გამოიწვიოს უნივერსიტეტის საქმიანობის ხანგძლივი შეფერხება ანდა პერსონალური ინფორმაციის გამჟღავნება. შეზღუდული ტიპის მონაცემები დაცულია სახელმწიფო კანონმდებლობით და სუბიექტებს შორის გაფორმებული კონფიდენციალურობის შეთანხმებებით (მაგ. თანამშრომელთა პირადი ინფორმაცია, სტუდენტთა აკადემიური მონაცემები, უნივერსიტეტის ფინანსური ინფორმაცია და სხვა). უსაფრთხოების ყველაზე მაღალი დონე უნდა იქნეს გამოყენებული შეზღუდული მონაცემებისათვის.

- **კერძო** - მონაცემთა არასანქცირებულმა გამჟღავნება დაკავშირებულია საშუალო დონის რისკებთან და მათი შეცვლამ ან განადგურებამ შეიძლება, ან არ გამოიწვიოს უნივერსიტეტის საქმიანობისათვის დროებითი შეფერხება. კერო ტიპის ინფორმაციას მიეკუთვნება უნივერისტეტის შიდა დოკუმენტბრუნვის სისტემაში არსებული მარეგულირებელი და მმართველობითი ტიპის ინფორმაცია. ჩვეულებრივ, უნივერსიტეტის ყველა მონაცემი, რომელიც არ არის აშკარად კლასიფიცირებული, როგორც შეზღუდული ან საჯარო მონაცემი უნდა მიკუთვნოს კერძო მონაცემებს და მათი დაცვა უნდა მოხდეს უსაფრთხოების საშუალო დონის მიხედვით.

- **საჯარო** - მონაცემთა არასანქცირებულმა გამჟღავნებამ, შეცვლამ ან განადგურებამ შეიძლება გამოიწვიოს დაკავშირებულია საფრთხის დაბალ რისკებთან. საჯარო მონაცემების მაგალითებია: განცხადებები, შეტყობინებები, კურსის სასწავლო განრიგი, პრესრელიზები, საინფორმაციო ბიულეტენი, გაზეთები, ჟურნალები, ვებ-გვერდები, სამეცნიერო ნაშრომები და სხვა. საჯარო მონაცემების დაცვისათვის საჭიროა უსაფრთხოების დაბალი დონე.

უნივერსიტეტის საინფორმაციო რესურსებთან მიწვდომა განისაზღვრება მომხმარებლის უფლებებით. მომხმარებელმა უნდა დაიცვას არა მხოლოდ უნივერსიტეტის, არამედ სხვა მომხმარებლებისა და მესამე პირების მიერ დაწესებული შეზღუდვები, რომლებიც არ ეწინააღმდეგება უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას.

სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ფიზიკური, ტექნიკური, პროცედურული და გარემოს უსაფრთხოების კონტროლის მექანიზმებით, რისთვისაც ახდენს ინფორმაციისა და მონაცემების ცენტრალიზებულად შენახვას, დაცვას, არქივირებისა და სარეზერვო ასლების შექმნას/შენახვას და ფორსმაჟორულ სიტუაციების შემთხვევაში მონაცემების აღდგენასა და მთლიანობას.

უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემები, როგორც პერსონალური კომპიუტერები, ასევე საკომუნიკაციო სისტემები უნდა იყოს დაცული ვირუსული და სხვა კიბერ-თავდასხმებისაგან.

უნივერსიტეტი პასუხს არ აგებს მომხმარებლების პირადი კომპიუტერებში ან ნებისმიერი სხვა უნივერსიტეტის სისტემის გარეთ ან/და სათანადო წესების დაუცველად შენახული ფაილებისა ან მონაცემების დაცვაზე, თუმცა უზრუნველყოფს მომხმარებლების ინფორმირებას რისკების შესახებ და მისი კომპეტენციების ფარგლებში უზრუნველყოფს მათ მხარდაჭერას.

7. საავტორო უფლებები

უნივერსიტეტი იზიარებს საქართველოს კანონის მოთხოვნებს საავტორო და მომიჯნავე უფლებების შესახებ[2].

უნივერსიტეტის კომპიუტერულ ქსელში არსებული პროგრამული უზრუნველყოფა და მონაცემთა ბაზები ეკუთვნის ან ლიცენზირებულია უნივერსიტეტის ან მესამე მხარის მიერ და დაცულია საავტორო უფლებებით, ლიცენზირებისა და ხელშეკრულებათა წესებითა და სხვა კანონებით. მომხმარებელი ვალდებულია პატივი სცეს და დაიცვას პროგრამული უზრუნველყოფის გამოყენებისა და განაწილების ლიცენზიების პირობები, რომელიც შეიცავს შემდეგი სახის აკრძალვას:

1. უნივერსიტეტის ქსელში გამოყენების მიზნით პროგრამების ასლის შექმნა ან უნივერსიტეტის ფარგლებს გარეთ მისი გავრცელება;
2. საავტორო უფლებებით დაცული ნამუშევრების არასანქცირებული ჩამოტვირთვა და საუნივერსიტეტო კომპიუტერულ ქსელში ან/და სხვა საინფორმაციო რესურსების საშუალებით გამოყენება;
3. მონაცემთა ან/და პროგრამების გაყიდვა;
4. პროგრამული უზრუნველყოფის გამოყენება არასასწავლო მიზნებისა ან/და ფინანსური მოგებისათვის;
5. პროგრამების (მაგ.: პროგრამული კოდის) ან მონაცემების მათი ავტორების / მფლობელების ნებართვის გარეშე საჯაროდ გამჟღავნება.

   უნივერსიტეტის ქსელთან დაკავშირებისას ყველა მომხმარებელი ვალდებულია დაიცვას ნამუშევრების საავტორო უფლებები, რომლებიც ხელშეკრულების შეთანხმების სახით ჩვეულებრივ განთავსებულია მომწოდებლის ვებგვერდზე. მომხმარებელი რომ არ დაეთანხმოს კონკრეტულ საავტორო უფლებებს, ეს მაინც არ ნიშნავს, რომ საავტორო უფლებები არ ვრცელდება ამ ნამუშევარზე.

2 მუხლები 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

საინფორმაციო-საკომუნიკაციო ტექნოლოგიების მართვის პროცედურები

2. მომხმარებლის ანგარიშის შექმნა და გაუქმება

უნივერსიტეტის კომპიუტერული რესურსებისა და ელექტრონული ფოსტის გამოყენებისათვის არსებობს მომხმარებელთა ჩვეულებრივი და განსაკუთრებული უფლებების (იხ. „მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა“) მქონე ანგარიშები.

განსაკუთრებული უფლებების მქონე (ადმინისტრატორი) მომხმარებელს განსაზღვრავს ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტის ხელმძღვანელი, ხოლო უნივერსიტეტის სტუდენტებისა, აკადემიურ და მოწვეულ პერსონალს, აგრეთვე დამხმარე სტრუქტურების თანამშრომლებს აქვს ჩვეულებრივი სამომხმარებლო ანგარიში

2.1. მომხმარებლის ანგარიშის შექმნა

ადამიანური რესურსების მართვის სამსახურის მიერ მოწოდებული ახალ თანამშრომელთა სიის თანახმად ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი ყოველი თანამშრომლისათვის ქმნის კომპიუტერულ და ელექტრონული ფოსტის ანგარიშს. ფაკულტეტის სასწავლო-სამეცნიერო აკადემიური პერსონალისათვის ფაკულტეტის ხელმძღვანელის წარდგინებით იქმნება სასწავლო/მასწავლი პროგრამების ანგარიში.

ყოველი ახალი სტუდენტისათვის მისი რეგისტრაციისთანავე იქმნება ელექტრონული ფოსტისა და სასწავლო/მასწავლი პროგრამების ანგარიშები.

2.2. ანგარიშების გაუქმება

ადამიანთა რესურსების სამსახურის მიერ გადმოცემული უნივერსიტეტიდან წასულ თანამშრომელთა სიის მიხედვით, ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური აუქმებს ამ თანამშრომელთა შესაბამის ანგარიშებს.

სტუდენტის სტატუსის ცვლილება გავლენას არ ახდენს ელექტრონული ფოსტის ანგარიშზე. უნივერსიტეტის დამთავრების ან სტატუსის შეწყვეტა/შეჩერების შემდეგ განისაზღვრება მისი ანგარიშით უნივერსიტეტის კომპიუტერულ რესურსებზე წვდომის შეზღუდული უფლებები.

3. პაროლის შექმნა

პაროლი ინფორმაციული და ქსელური უსაფრთხოების მნიშვნელოვანი კომპონენტია და მომხმარებლის სახელი (User) და პაროლი (Password) ერთად ემსახურება მომხმარებლის ნამდვილობის შემოწმებას, აგრეთვე მის პერსონალური და უნივერსიტეტის კორპორატიულ ინფორმაციის დაცვასა და ამართვას,

პაროლი წარმოადგენს ტექსტურ სიდიდეს და შექმნისთვის უნდა იქნეს გათვალისწინებული, შემდეგი პარამეტრები:

1. უნდა შეიცავდეს ლათინური ანბანის დიდ და პატარა სიმბოლოებს (მაგ.: a-z, A-Z);
2. უნდა შეიცავდეს ციფრს, არითმეტიკული მოქმედების ან/და სხვა სიმბოლოებს (მაგ.:
3. 0-9, @#$%^&*()_+|~- =\` {}[]:";'<>?,./);
4. სიგრძე (სიმბოლოთა რაოდენობა) უნდა იყოს არანაკლებ 8 ალფავიტურ-ციფრული სიმბოლო;

5. არ უნდა იყოს გამოყენებული რაიმე სიტყვა: გვარი, სახელი, ქალაქები სახელები, კომპიუტერული ტერმინები, დაბადების თარიღები, ტელეფონის ნომერი, დაწესებულებების სახელები და სხვა;;

6. პაროლის გამოყენება და მართვა

ყოველი მომხმარებელი ანგარიშის შექმნისთანავე ღებულობს ადმინისტრატორისგან ერთჯერად პაროლს და ვალდებულია შეცვალოს იგი პირველივე გამოყენების დროს.

პაროლის გამოყენებისას ყოველმა მომხმარებელმა უნდა გაითვალისწინოს შემდეგი საკითხები:

- დაუყონებლივ შეცვალოს სისტემის ადმინისტრატორისაგან მიღებული დროებითი პაროლი;
- არ გამოიყენოს ერთი და იგივე პაროლი უნივერსიტეტის ანგარიშებისა და სხვა ანგარიშებისათვის (მაგ., პირადი ელექტრონული ფოსტის ანგარიში);
- არ გაუზიაროს უნივერსიტეტის ანგარიშების პაროლების სხვას, მათ შორის ადმინისტრაციის წარმომადგენლებს, თანამშრომლებსა ან კოლეგებს (მაგ., შვებულებაში ყოფნის დროსაც კი), ოჯახის წევრებს;
- ქაღალდზე ანდა ელექტრული ფორმით ჩანაწერის სახით არ შეინახოს პაროლი;
- არ გააგზავნოს პაროლი ელექტრონული ფოსტით ან ნებისმიერი სხვა კომუნიკაციური საშუალებით (მაგ., მობილურით);
- ბრაუზერებში არ გამოიყენოს „დამიმახსოვრე“ პარამეტრი;
- სამუშაო ადგილზე არ ყოფნის დროს არ დატოვოს პაროლით დაცული რესურსები (ელექტრონული ფოსტა, ელექტრონული დეკანატი ან სხვა) გახსნილ მდგომარეობაში.

პაროლის დავიწყების, აგრეთვე გამჟღავნებისა, ანდა სხვა პირების მიერ არასანქცირებული წვდომის მოპოვების მცდელობაზე ეჭვის შემთხვევა შემთხვევაში დაუყონებლივ მიმართოს ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტის თანამშრომელს რომელიც მოაწვდის დროებით პაროლს.

გარკვეულ შემთხვევებში ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტის თანამშრომელმა შეიძლება მოითხოვოს მომხმარებლის პაროლი მისი დახმარების მოთხოვნის შემთხვევაში, თუმცა მას შემდეგ რაც აღმოიფხვრება პრობლემა პაროლი ექვემდებარება ცვლილებას.

4. უნივერსიტეტის ელექტრონული ფოსტა

ელექტრონული ფოსტა, რომელიც ფუნქციონირებს @eeu.edu.ge დომენით წარმოადგენს უნივერსიტეტის საკუთრებასა და შეიძლება გამოყენებულ იქნეს მხოლოდ სამსახურებრივი მიზნებით და წარმოადგენს სტუდენტებისა და თანამშროლობებისათვის შიდა და გარე კომუნიკაციის საშუალებას.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის თანახმად [3] უნივერსიტეტის თანამშრომლებისა და სტუდენტების ელექტრონული ფოსტის ინდივიდუალური ანგარიშიდან განხორციელებული მიმოწერა წარმოადგენს მათ პირად ინფორმაციას და არ ექვემდებარება

[3] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ – https://matsne.gov.ge/ka/document/view/1561437

შინაარსობრივ მონიტორინგს.

ელექტრონული ფოსტის სისტემის მუშაობასთან დაკავშირებული ნებისმიერი კითხვით მომხმარებლებმა უნდა მიმართოს თავის უშუალო ხელმძღვანელსა და/ან უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტს.

ელექტრონული ფოსტის გამოყენებისას დაუშვებელია:

- უხამსობის, შეურაცხყოფისა და ცილისწამების გავრცელება, თაღლითობა, დაშინება, გაყალბება, უკანონო პირამიდული სქემების შექმნა ან კომპიუტერული საზიანო პროგრამების გავრცელება და სხვა;
- ანგარიშის მფლობელის ან სხვა პირის ნებართვის გარეშე ელექტრონული ფოსტის ანგარიშების ან ფაილების დათვალიერება, მათი ასლის შექმნა, შეცვლა ან წაშლა;
- საეჭვო მისამართებიდან გამოგზავნილი შეტყობინების თანდართული დოკუმენტების, რომლებიც არიან ვირუსებისა და საზიანო პროგრამების გავრცელების პირდაპირი წყაროები, გახსნა;
- ელექტრონული ფოსტის ანგარიშის საკუთარი პაროლების გაზიარება სხვა პიროვნებათათვის ან სხვა პირის ანგარიშის პაროლის გაგების მცდელობა;
- კომერციული საქმიანობის, პოლიტიკური კამპანიის ფარგლებში წერილების გავრცელებისა და ელექტრონული ფოსტის გამოყენება.

4.1. ელექტრონული ფოსტის მისამართი

უნივერსიტეტში გამოიყენება შემდეგი ტიპის ელექტრონულ ფოსტის ანგარიში:

- უნივერსიტეტის თანამშრომლებისა და სტუდენტების ინდივიდუალური ანგარიში. ანგარიში ფორმირდება სახელისა და გვარის კომბინაციით, იმ შემთხვევაში თუ აღნიშნული კომბინაცია დაკავებულია, ემატება რიგითი ნომერი (დარეგისტრირების თანმიმდევრობის მიხედვით);ხოლო სტუდენტებისათვის ანგარიში ფორმირდება ბაზის 4 ნიშნა ID-ის საშუალებით, დამთხვევის შემთხვევაში წინ ემატება G ან E ასო.
- ცალკეული სტრუქტურული ერთეულის (ფაკულტეტი, დეპარტამენტი და ა. შ.), კვლევით, სამეცნიერო, კულტურულ და სოციალური პროექტების და სხვა სპეციალური საფოსტო ანგარიშები ფორმირდება შესაბამის სამსახურებთან შეთანხმებით და მათი მიმართვის საფუძველზე;

4.2. ელექტრონული ფოსტის ანგარიშის შეჩერება ან გაუქმება

ელექტრონული ფოსტის ანგარიშის ფუნქციონირების დროებით შეჩერება ხდება შემდეგ შემთხვევებში:

1. უნივერსიტეტის სტუდენტებისა და თანამშრომლების მიერ ზემოაღნიშნული პოლიტიკის დარღვევა;
2. თანამშრომლისათვის მისი უნივერისტეტიდან გათავისუფლება;
3. სტუდენტისათვის სტატუსის შეწყვეტა ან სხვა უნივერსიტეტში გადასვლა;
4. ცალკეული სტრუქტურული ერთეულის ლიკვიდაცია/რეორგანიზაცია;
5. უნივერსიტეტის ელექტრონული ფოსტის არამიზნობრივი გამოყენების ფაქტის დადგენის მიზნით შიდა მოკვლევის წარმოებისას;

6. ამ პოლიტიკითა და საქართველოს კანონმდებლობით აკრძალული ინფორმაციის გავრცელება;
7. მესამე პირის მიერ ანგარიშზე წვდომის ფაქტის გამოვლენა;
8. საინფორმაციო სისტემაში და ქსელურ ინფრასტრუქტურაში ტექნიკური პრობლემების წარმოქნის შეთხვევაში;

ტექნიკური პრობლემების წარმოქნის შეთხვევაში უნივერსიტეტის ელექტრონული ფოსტის ანგარიშის ფუნქციონირების დროებითი შეჩერების შესახებ ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი ვალდებულია შეატყობინოს, როგორც ანგარიშის მფლობელს, ასევე მის უშუალო ხელმძღვანელს. შეზღუდვა იხსნება მისი გამომწვევი მიზეზების აღმოფხვრის შემდეგ და ამის შესახებ ეცნობება, როგორც ანგარიშის მფლობელს, ასევე მის უშუალო ხელმძღვანელს.

შესაძლებელია მომხმარებლის ელექტრონული ფოსტასთან მოკლევადიანი წვდომა, მისი თანხმობის შემთხვევაში, რათა განსაკუთრებულ შემთხვევებში:

- უზრუნველყოფილი იყოს საუნივერსიტეტო საქმიანობის უწყვეტობა (მაგ., ინფორმაციის მიღების საჭიროების შემთხვევაში მაშინ, როცა მომხმარებელი მიუწვდომელია);
- მოხდეს სისტემასთან დაკავშირებული ტექნიკური პრობლემების დიაგნოსტიკა და აღმოფხვრა;

დაუშვებელია ფოსტის ანგარიშის სრულად წაშლა.

თანამშრომლის ელექტრონული ფოსტის ანგარიში, რომელთანაც შეწყდება უნივერსიტეტთან ხელშეკრულება, უნდა შეჩერდეს, ხოლო ყოფილ თანამშრომლის მიერ კი ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტისათვის თავის ელექტრონული ფოსტის პაროლის გადაცემა, რათა საჭიროების შემთხვევაში შესაძლებელი იყოს მის ანგარიშთან წვდომა.

უნივერსიტეტის კომპიუტერული ქსელების მართვა

უნივერსიტეტის კომპიუტერული ქსელი შედგება სადენიანი და უსადენო ქსელებში მართვისა და მონაცემთა გადაცემის ინფრასტუქტურისაგან, ასევე მონაცემთა ბაზებისა და აპლიკაციების მართვის სერვერებისა, რომელთა შეუფერხებელ მუშაობასა და ადმინისტრირებას უზრუნველყოფს ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი.

ქსელური ინფრასტრუქტურის ტექნიკური ან პროგრამული განახლება და რაიმე სხვა გეგმიური სერვისული სამუშაოები, რომელიც გამოიწვევს კომპიუტერული ქსელის მუშაობის შეფერხებას უნდა განხორციელდეს არასამუშაო საათებში და 24 საათით ადრე ეცნობოს ყველა მომხმარებლებს.

4.3. IP მისამართის მართვა

კომპიუტერული მოწყობილობების ინტერნეტ მისამართების (IP) განაწილება ხდება ქსელში ჩართული სერვერის მეშვეობით (DHCP პროტოკოლის გამოყენებით), რომლის მართვას, მხარდაჭერასა და დოკუმენტირებას ახორციელებს უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი.

უნივერსიტეტში ქსელში ჩართულ ყოველ მოწყობილობებს შეიძლება მიენიჭოს დინამიკური ან სტატიკური IP მისამართი, მათ შორის:

- გამონაკლისის სახით, სტატიკური IP მისამართების მინიჭების შესაძლებელია ქსელური

ინფრასტრუქტურის გამართული ფუნქციონირებასა და უსაფრთხოების მიზნით.

- დინამიკურად IP მისამართების მინიჭება ხდება საუნივერსიტეტო ქსელში ჩართული ყველა კომპიუტერულ და მობილურ მოწყობილობისთვის.

4.4. ქსელური მარშრუტიზატორის მართვა და უსაფრთოხება

უნივერსიტეტის ქსელში ჩართული ყველა მარშრუტიზატორის სათანადო მონტაჟზე და ინსტალაციაზე, ასევე მათ უსაფრთხოებაზე, მართვაზე, მონიტორინგისა და პერიოდული აუდიტის პასუხიმგებელია ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტი.

ქსელური მარშრუტიზატორი უნდა შეესაბამებოდეს უსაფრთხოების ფართედ გამოყენებად სტანდარტებს.

მარშრუტიზატორი მუშაობისას უნდა უზრუნველყოფილი იქნეს შემდეგი:

- წვდომის პაროლი უნდა ინახებოდეს დაშიფრული ფორმით;
- მართვისა და მონიტორინგისთვის უნდა გამოიყენებოდეს სტანდარტიზებული SNMP პროტოკოლი;
- მარშრუტიზატორის დაშორებული კონფიგურაციისათვის უნდა გამოიყენებოდეს დაშიფრული (ssh) არხი;

ქსელური მარშრუტიზატორის მუშაობისა და უსაფრთხოების მონიტორინგი უნდა მიმდინარეობდეს 24/365 რეჟიმში, ხოლო არანაკლებ წელიწადში ყოველ უნდა ხორციელდებოდეს უსაფრთხოებისა და წარმადობის პერიოდული აუდიტი, რომლის ანგარიშები მიეწოდება რექტორს.

4.5. უსადენო კავშირის მართვა

უნივერსიტეტის უსადენო ქსელების მართვა, მონიტორინგი და ექსპლუატაცია ხდება ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტის მიერ.

უსადენო ქსელში დაშვება შეიძლება იყოს თავისუფალი ან შეზღუდული.

- თავისუფალი დაშვების უსადენო ქსელის პაროლი შეიძლება გაენდოს ნებისმიერ მსურველს, დაიწეროს საინფორმაციო დაფაზე ან განთავსდეს ნებისმიერ თვალსაჩინო ადგილზე.
- შეზღუდული წვდომის უსადენო ქსელის პაროლი ეცნობება მხოლოდ მათ, რომელთაც სამსახურეობრივი საქმიანობიდან გამომდინარე ჭირდებათ აღნიშნულ ქსელთან წვდომა.

მიუხედავად იმისა უსადენო ქსელი არის შეზღუდული თუ თავისუფალი დაშვების მასთან წვდომა უნდა ხდებოდეს WPA2/PSK ტექნოლოგიით და AES შიფრირებით შესაბამისი პაროლის გამოყენებით, რათა მაქსიმალურად იქნას დაცული აღნიშნულ ქსელში გადაცემული ინფორმაცია არასანქცირებული წვდომისგანა.

4.6. კომპიუტერული ქსელის მონიტორინგი

უნივერსიტეტის ქსელში ჩართული ყველა კომპიუტერული და საკომუნიკაციო საშუალება ექვემდებარება წინამდებარე პოლიტიკას, იმის და მიუხედავად არის თუ არა ეს მოწყობილობა უნივერსიტეტის საკუთრება.

თუ არსებობს წინამდებარე პოლიტიკის დარღვევის ფაქტები, უნივერსიტეტის

ინფორმაციული ტექნოლოგიებთან და კომპიუტერულ ინფრასტრუქტურასთან არასანქციონირებული წვდომის ანდა ბოროტად გამოყენების ეჭვი, აგრეთვე რათა გამოავლინოს კომპიუტერული ქსელის ტექნიკური პრობლემები, ვირუსებისა და სხვა საზიანო პროგრამების არსებობა უნივერსიტეტი იტოვებს უფლებას, შინაარსობრივი მონიტორინგის გარეშე შეამოწმოს და შეისწავლოს მის კომპიუტერულ სისტემებისა და ქსელების ყველა ელემენტი, მათ შორის ინდივიდუალური ანგარიშის შემცველი ფაილები და ინფორმაცია.

უნივერსიტეტის ქსელის, ინტერნეტ კავშირისა ან უნივერსიტეტის კომპიუტერული რესურსების მონიტორინგი შეუძლია განახორციელოს მხოლოდ ინფორმაციული ტექნოლოგიების მართვის დეპარტამენტს. დაუშვებელია სხვა ყველა მომხმარებლის მიერ ქსელის მონიტორინგის მცდელობა.

უნივერსიტეტის ქსელისა და ინტერნეტის შემოწმების უფლებამოსილმა პერსონალმა უნივერსიტეტის ადმინისტრაციის ნებართვის გარეშე არ უნდა გაამჟღავნოს, ანდა გადასცეს მესამე პირებს ქსელის მონიტორინგის პროცესში მიღებული ინფორმაცია.