დამტკიცებულია:

ა(ა)იპ „გიორგი მთაწმინდელის სახელობის

გალობის უნივერსიტეტის“ რექტორის 2024 წლის 02 სექტემბრის

№ო/27 ბრძანებით (დანართი 1)

ა(ა)იპ „გიორგი მთაწმინდელის სახელობის გალობის უნივერსიტეტის“ ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები

მუხლი 1. ზოგადი დებულებები

1.წინამდებარე დოკუმენტი მოიცავს ყველა აუცილებელ პრინციპსა და პროცედურას, რომელიც უზრუნველყოფს ა(ა)იპ „გიორგი მთაწმინდელის სახელობის გალობის უნივერსიტეტში“ (შემდგომ ტექსტში - „უნივერსიტეტი“) ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის, მომსახურების, რისკების მართვისა და უსაფრთხოების მაქსიმალურ ეფექტურობას.

2. უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები (შემდგომ ტექსტში - „წესი“) მიმართულია გალობის უნივერსიტეტის მმართველობით, საგანმანათლებლო, სამეცნიერო-კვლევით და შემოქმედებით პროცესებში კომპიუტერული და საინფორმაციო რესურსების ეფექტიან და უსაფრთხო გამოყენებაზე, გალობის უნივერსიტეტის საინფორმაციო ტექნოლოგიების მომხმარებლის უფლება-მოვალეობების განსაზღვრასა და ინფორმაციულ უსაფრთხოებაზე.

მუხლი 2. პოლიტიკის მიზანი

უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა განსაზღვრავს უნივერსიტეტის მმართველობით, საგანმანათლებლო, სამეცნიერო-კვლევით და შემოქმედებით პროცესებში, კომპიუტერული და საინფორმაციო რესურსების გამოყენების საკითხებში ზოგად მიდგომებსა და წესებს, რომლის საფუძველზეც ხდება ინფორმაციული ტექნოლოგიების მართვის პროცედურების ფორმირება, მათ შორის, სისტემების უსაფრთხო გამოყენების მიზნით.

მუხლი 3. პოლიტიკის მოქმედების სფერო

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა ვრცელდება ადმინისტრაციულ/დამხმარე, აკადემიურ/მოწვეულ პერსონალზე, სპეციალისტებსა და სტუდენტებზე, ასევე, ყველა იმ პირზე, ვინც ჩართულია უნივერსიტეტის მმართველობით,

საგანმანათლებლო და სამეცნიერო-კვლევით, შემოქმედებით პროცესებში და რომელსაც გააჩნია ლეგიტიმური წვდომა უნივერსიტეტის კომპიუტერულ, ქსელურ და საინფორმაციო რესურსებთან.

მუხლი 4. ზოგადი პრინციპები

უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ზოგადი პრინციპებია:

ა) კონფიდენციალურობა:

კონფიდენციალურობა უზრუნველყოფს, რომ პერსონალური, აკადემიური და ორგანიზაციული მონაცემები დაცული იყოს არასანქცირებული წვდომისგან, ან გამოყენებისგან. ეს ხელს უწყობს უნივერსიტეტის რეპუტაციის შენარჩუნებას, მომხმარებელთა ნდობის გაღრმავებასა და მონაცემთა დაცვის სამართლებრივი მოთხოვნების დაკმაყოფილებას;

ბ) უსაფრთხოება:

უსაფრთხოების დაცვა მნიშვნელოვანია მონაცემთა და სისტემების ხელშეუხებლობის უზრუნველსაყოფად, რაც ამცირებს კიბერთავდასხმების, მონაცემთა დაკარგვისა და სისტემური ჩავარდნების რისკებს. უსაფრთხოება ასევე ხელს უწყობს უნივერსიტეტის ინფრასტრუქტურის გამართულ მუშაობასა და მომსახურების უწყვეტობას;

გ) ინფორმაციის გამოყენება:

უნივერსიტეტის ტექნოლოგიური რესურსების ეფექტური და მიზანმიმართული გამოყენება აუცილებელია ოპერაციების ეფექტურობისთვისა და რესურსების არასათანადო გამოყენების რისკის შესამცირებლად. ეს პოლიტიკა უზრუნველყოფს, რომ რესურსები გამოყენებულია მხოლოდ აკადემიური და ადმინისტრაციული მიზნებისთვის, რაც ორგანიზაციის მიზნების მისაღწევად ხელსაყრელია;

დ) ხელმისაწვდომობა:

შეუზღუდავი და დროული წვდომა უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემებზე, უზრუნველყოფს თანამშრომლების მუშაობის ეფექტურობასა და ინფორმაციის სწორი დროში მიღებას. ეს პრინციპი აუცილებელია თანამშრომლობის, სწავლისა და კვლევის პროცესების სრულყოფილად ფუნქციონირებისთვის;

ე) ანგარიშვალდებულებითობა:

ანგარიშვალდებულება თანამშრომლებს უბიძგებს იზრუნონ IT რესურსების დაცვისა და განვითარების პროცესში მონაწილეობაზე. ეს უზრუნველყოფს რესურსების გამოყენების გამჭვირვალობას და ხელს უწყობს სამუშაო გარემოს გაუმჯობესებას ტექნოლოგიების ეფექტურად გამოყენების გზით;

ვ) სისტემების ხელშეწყობა და განახლება:

საინფორმაციო ტექნოლოგიების სისტემების მუდმივი განახლება და მხარდაჭერა აუცილებელია მათი ეფექტურობის, უსაფრთხოებისა და თანამედროვე სტანდარტებთან შესაბამისობის უზრუნველსაყოფად. ამ პრინციპის დაცვა ხელს უწყობს უნივერსიტეტის მუშაობის უწყვეტობას, რესურსების მაქსიმალურ ეფექტურ გამოყენებასა და მონაცემების დაცულობას.

მუხლი 5. ინფორმაციული უსაფრთხოება

1. საინფორმაციო-საკომუნიკაციო სისტემის ადმინისტრატორის (ინფორმაციული ტექნოლოგიების სამსახურის უფროსი) გარდა ყველა მომხმარებელს, გალობის უნივერსიტეტის რექტორის ნებართვის გარეშე, ეკრძალება საინფორმაციო რესურსის მონიტორინგი, ასევე სისტემური პარამეტრების ცვლილება. ანალოგიური მიდგომაა საუნივერსიტეტო მართვის, სწავლებისა და სამეცნიერო მონაცემთა ბაზებთან, პროგრამებთან და აპლიკაციებთან წვდომის თვალსაზრისითაც

2. გალობის უნივერსიტეტი არ ახდენს მომხმარებლების მიერ კომპიუტერულ ქსელში გადაცემული მასალის შემოწმებას, ან/და რაიმე ფორმით შეზღუდვას. 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 ეცნობებათ მათ.

მუხლი 6. მონაცემთა დაცვა

1. სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ტექნიკური, უსაფრთხოების კონტროლის მექანიზმებით.

2. 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.

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

4. 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.

5. 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.

6. 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.

7. გალობის უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემები, როგორც პერსონალური კომპიუტერები, ასევე საკომუნიკაციო სისტემები უნდა იყოს დაცული ვირუსული და სხვა კიბერთავდასხმებისაგან.

8. გალობის 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.

მუხლი 7. მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა

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

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

3. 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.

მუხლი 8. მომხმარებელთა უფლება-მოვალეობები

1. საუნივერსიტეტო საზოგადოების ყველა წევრსა და ჯგუფს, გააჩნიათ შესაძლებლობა შეზღუდვების გარეშე ჰქონდეთ წვდომა უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემებთან.

2. უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემების, 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 საინფორმაციო ტექნოლოგიების სამსახური.

3. უნივერსიტეტის მფლობელობაში, ან ზედამხედველობის ქვეშ მყოფი საინფორმაციო-საკომუნიკაციო ტექნიკა მომხმარებელს დროებით სარგებლობაში გადაეცემა სამუშაო, ან/და სასწავლო ხელშეკრულების მოქმედების პერიოდში (შემდგომ ტექსტში - „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, ეს ტექნიკა დაუშვებელია გამოყენებულ იქნეს რომელიმე პიროვნების ცილისწამებისა და შეურაცხყოფის მიზნით.

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

მუხლი 9. ინფორმაციული უსაფრთხოება

უნივერსიტეტის საინფორმაციო-საკომუნიკაციო სისტემები იმგვარად უნდა იყოს მოწყობილი, რომ უზრუნველყოს სამეწარმეო, სამუშაო, პერსონალური, პირადი ინფორმაციისა და მონაცემების დაცულობა და მთლიანობა, რისთვისაც ნებისმიერ მომხმარებელს:

ა) არ შეეძლოს მესაკუთრის თანხმობის გარეშე: დაათვალიეროს, შექმნას ასლი, შეცვალოს ან წაშალოს ელექტრონული ფაილები და მონაცემთა ბაზებში ინფორმაცია;

ბ) მოახდინოს სისტემური პარამეტრების ცვლილება;

გ) სათანადო ნებართვის გარეშე მიიღოს წვდომა საუნივერსიტეტოს მართვის, სწავლებისა და სამეცნიერო მონაცემთა ბაზებთან, პროგრამებთან და აპლიკაციებთან;

დ) სათანადო ნებართვის გარეშე მესამე პირებს არ გადასცენ უნივერსიტეტის საინფორმაციო-საკომუნიკაციო რესურსებზე დაცული ინფორმაცია, თავისი, ან/და სხვისი მომხმარებლის ანგარიშის პარამეტრები და პერსონალური მონაცემების შემცველი ინფორმაცია, აგრეთვე მონაცემები, რომელიც წარმოადგენს უნივერსიტეტისთვის საკუთრებას და არის კონფიდენციალური, კომერციული საიდუმლოება ან/და დაცულია საავტორო უფლებით.

მუხლი 9. საინფორმაციო ტექნოლოგიების მართვის პროცედურები

1. უნივერსიტეტის კომპიუტერული რესურსებისა და ელექტრონული ფოსტის გამოყენებისათვის არსებობს მომხმარებელთა ჩვეულებრივი და განსაკუთრებული უფლებების მქონე (ადმინისტრატორი) ანგარიშები.

2. განსაკუთრებული უფლებების მქონე (ადმინისტრატორი) მომხმარებელს განსაზღვრავს საინფორმაციო ტექნოლოგიების სამსახურის ხელმძღვანელი, ხოლო უნივერსიტეტის სტუდენტებისა, აკადემიურ და მოწვეულ პერსონალს, აგრეთვე სტრუქტურული ერთეულების თანამშრომლებს აქვს ჩვეულებრივი სამომხმარებლო ანგარიში.

3. ადმინიტრაციულ სტრუქტურული ერთეულებისთვის მომხმარებლის ანგარიშის შექმნა ხდება აინფორმაციო ტექნოლოგიების სამსახურის მიერ, ადამიანური რესურსების მართვისა და საქმისწარმოების სამსახურის მიერ მოწოდებული ახალ თანამშრომელთა სიის თანახმად.

4. საინფორმაციო ტექნოლოგიების სამსახური ყოველი თანამშრომლისათვის ქმნის კომპიუტერული და ელექტრონული ფოსტის ანგარიშს.

5. ფაკულტეტის აკადემიური/მოწვეული პერსონალისთვის და სპეციალისტებისთვის ფაკულტეტის დეკანის წარდგინებით საინფორმაციო ტექნოლოგიების სამსახურის მიერ იქმნება პროგრამების (ელ.ფოსტის) ანგარიში. ასევე, ყოველი ახალი სტუდენტისთვის მისი რეგისტრაციისთანავე იქმნება ელექტრონული ფოსტისა და სასწავლო/მასწავლი პროგრამების ანგარიშები.

6. საინფორმაციო ტექნოლოგიების სამსახურის მიიერ ანგარიშების გაუქმება ხდება ადამიანური რესურსების მართვისა და საქმისწარმოების სამსახურის მიერ გადმოცემული უნივერსიტეტიდან წასული თანამშრომელთა სიის მიხედვით. 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.

მუხლი 11. პაროლის შექმნა

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

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

ა) უნდა შეიცავდეს ლათინური ანბანის დიდ და პატარა სიმბოლოებს (მაგ.: a-z, A-Z);

ბ) უნდა შეიცავდეს ციფრს, არითმეტიკული მოქმედების ან/და სხვა სიმბოლოებს (მაგ.: 0-9, @#$%^&*()_+|~- =\` {}[]:";'<>?,./);

გ) სიგრძე (სიმბოლოთა რაოდენობა) უნდა იყოს არანაკლებ 8 ალფავიტურ-ციფრული სიმბოლო;

დ) არ უნდა იყოს გამოყენებული რაიმე სიტყვა: გვარი, სახელი, ქალაქების სახელები, კომპიუტერული ტერმინები, დაბადების თარიღები, ტელეფონის ნომერი, დაწესებულებების სახელები და სხვა.

მუხლი 12. პაროლის გამოყენება და მართვა

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

2. პაროლის გამოყენებისას ყოველმა მომხმარებელმა უნდა გაითვალისწინოს შემდეგი საკითხები:

ა) დაუყონებლივ შეცვალოს სისტემის ადმინისტრატორისაგან მიღებული დროებითი პაროლი;

ბ) არ გამოიყენოს ერთი და იგივე პაროლი უნივერსიტეტის ანგარიშებისა და სხვა ანგარიშებისათვის (მაგ., პირადი ელექტრონული ფოსტის ანგარიში);

გ) არ გაუზიაროს უნივერსიტეტის ანგარიშების პაროლები სხვას, მათ შორის ადმინისტრაციის წარმომადგენლებს, თანამშრომლებსა, ან კოლეგებს (მაგ., შვებულებაში ყოფნის დროსაც კი), ოჯახის წევრებს;

დ) ქაღალდზე, ან/და ელექტრული ფორმით ჩანაწერის სახით არ შეინახოს პაროლი;

ე) არ გააგზავნოს პაროლი ელექტრონული ფოსტით, ან ნებისმიერი სხვა კომუნიკაციური საშუალებით (მაგ., მობილურით);

ვ) ბრაუზერებში არ გამოიყენოს „დამიმახსოვრე“ პარამეტრი;

ზ) სამუშაო ადგილზე არ ყოფნის დროს არ დატოვოს პაროლით დაცული რესურსები (ელექტრონული ფოსტა, ელექტრონული დეკანატი ან სხვა) გახსნილ მდგომარეობაში;

თ) პაროლის დავიწყების, აგრეთვე გამჟღავნებისა, ანდა სხვა პირების მიერ არასანქცირებული წვდომის მოპოვების მცდელობაზე ეჭვის შემთხვევა შემთხვევაში დაუყონებლივ მიმართოს საინფორმაციო ტექნოლოგიების სამსახურს, რომელიც მოაწვდის დროებით პაროლს;

ი) გარკვეულ შემთხვევებში საინფორმაციო ტექნოლოგიების სამსახურის თანამშრომლემა შეიძლება მოითხოვოს მომხმარებლის პაროლი მისი დახმარების მოთხოვნის შემთხვევაში, თუმცა მას შემდეგ რაც აღმოიფხვრება პრობლემა პაროლი ექვემდებარება ცვლილებას.

მუხლი 13. ელექტრონული ფოსტის ანგარიშის შეჩერება ან გაუქმება

1. ელექტრონული ფოსტის ანგარიშის ფუნქციონირების დროებით შეჩერება ხდება შემდეგ შემთხვევებში:

ა) უნივერსიტეტის სტუდენტებისა და თანამშრომლების მიერ ზემოაღნიშნული პოლიტიკის დარღვევა;

ბ) თანამშრომლისთვის მისი უნივერისტეტიდან გათავისუფლება (შრომითი ხელშეკრულების შეწყვეტა);

გ) სტუდენტისათვის სტატუსის შეწყვეტა, ან სხვა უნივერსიტეტში გადასვლა;

დ) ცალკეული სტრუქტურული ერთეულის ლიკვიდაცია/რეორგანიზაცია;

ე) უნივერსიტეტის ელექტრონული ფოსტის არამიზნობრივი გამოყენების ფაქტის დადგენის მიზნით შიდა მოკვლევის წარმოება;

ვ) ამ პოლიტიკითა და საქართველოს კანონმდებლობით აკრძალული ინფორმაციის გავრცელება;

ზ) მესამე პირის მიერ ანგარიშზე წვდომის ფაქტის გამოვლენა;

თ) საინფორმაციო სისტემაში და ქსელურ ინფრასტრუქტურაში ტექნიკური პრობლემების წარმოქმნა.

2. ტექნიკური პრობლემების წარმოქნის შეთხვევაში უნივერსიტეტის ელექტრონული ფოსტის ანგარიშის ფუნქციონირების დროებითი შეჩერების შესახებ საინფორმაციო ტექნოლოგიების სამსახური ვალდებულია შეატყობინოს, როგორც ანგარიშის მფლობელს, ასევე მის უშუალო ხელმძღვანელს.

3. 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, შემდეგ შემთხვევებში, რათა:

ა) უზრუნველყოფილი იყოს საუნივერსიტეტო საქმიანობის უწყვეტობა (მაგ., ინფორმაციის მიღების საჭიროების შემთხვევაში მაშინ, როცა მომხმარებელი მიუწვდომელია);

ბ) მოხდეს სისტემასთან დაკავშირებული ტექნიკური პრობლემების დიაგნოსტიკა და აღმოფხვრა;

გ) არ მოხდეს ფოსტის ანგარიშის სრულად წაშლა.

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

მუხლი 14. უნივერსიტეტის კომპიუტერული ქსელების მართვა

1. უნივერსიტეტის კომპიუტერული ქსელი შედგება სადენიანი და უსადენო ქსელებში მართვისა და მონაცემთა გადაცემის ინფრასტუქტურისაგან, ასევე მონაცემთა ბაზებისა და აპლიკაციების მართვის სერვერებისგან, რომელთა შეუფერხებელ მუშაობასა და ადმინისტრირებას უზრუნველყოფს საინფორმაციო ტექნოლოგიების სამსახური.

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

მუხლი 15. IP მისამართის მართვა

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

2. უნივერსიტეტში ქსელში ჩართულ ყოველ მოწყობილობას შეიძლება მიენიჭოს დინამიკური, ან სტატიკური IP მისამართი, მათ შორის:

ა) გამონაკლისის სახით, სტატიკური IP მისამართების მინიჭების შესაძლებელია ქსელური ინფრასტრუქტურის გამართული ფუნქციონირებასა და უსაფრთხოების მიზნით.

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

მუხლი 16. ქსელური მარშრუტიზატორის მართვა და უსაფრთოხება

1. უნივერსიტეტის ქსელში ჩართული ყველა მარშრუტიზატორის სათანადო მონტაჟზე და ინსტალაციაზე, ასევე მათ უსაფრთხოებაზე, მართვაზე, მონიტორინგისა და პერიოდული აუდიტის პასუხიმგებელია საინფორმაციო ტექნოლოგიების სამსახური.

2. ქსელური მარშრუტიზატორი უნდა შეესაბამებოდეს უსაფრთხოების ფართედ გამოყენებად სტანდარტებს.

3. მარშრუტიზატორი მუშაობისას უზრუნველყოფილი უნდა იქნეს შემდეგი:

ა) წვდომის პაროლი უნდა ინახებოდეს დაშიფრული ფორმით;

ბ) მართვისა და მონიტორინგისთვის უნდა გამოიყენებოდეს სტანდარტიზებული SNMP პროტოკოლი;

გ) მარშრუტიზატორის დაშორებული კონფიგურაციისათვის უნდა გამოიყენებოდეს დაშიფრული (ssh) არხი.

მუხლი 17. უსადენო კავშირის მართვა

1. უნივერსიტეტის უსადენო ქსელების მართვა, მონიტორინგი და ექსპლუატაცია ხდება საინფორმაციო ტექნოლოგიების სამსახურის მიერ.

2. 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.

3. შეზღუდული წვდომის უსადენო ქსელის პაროლი ეცნობება მხოლოდ მათ, რომელთაც სამსახურეობრივი საქმიანობიდან გამომდინარე ჭირდებათ აღნიშნულ ქსელთან წვდომა.

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

მუხლი 18. დასკვნითი დებულებები

1.წესი მტკიცდება რექტორის აქტით.

2.წესში შესატან ცვლილებებსა და დამატებებს შეიმუშავებს ინფორმაციული ტექნოლოგიების სამსახური და ამტკიცებს რექტორი.

3.წესი ამოქმედდეს დამტკიცებისთანავე.