ავიცენა

ბათუმის სამედიცინო უნივერსიტეტი

„დამტკიცებულია“
შპს ,,ავიცენა - ბათუმის სამედიცინო უნივერსიტეტის”
პარტნიორთა საერთო კრების 2022 წლის 29 ივლისის
№ 01-03/02 ოქმის
დანართი №3

ავიცენა - ბათუმის სამედიცინო უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

2022

სარჩევი

მუხლი 1. რეგულირების სფერო

1.1. წინამდებარე პოლიტიკა განსაზღვრავს უმაღლესი საგანმანათლებლო დაწესებულების - შპს „ავიცენა - ბათუმის სამედიცინო უნივერსიტეტის“ (შემდეგში „ავიცენა” ან „უნივერსიტეტი”) ინფორმაციული ტექნოლოგიების და მათი გამოყენებით ინფორმაციის შეგროვების, დამუშავებისა და გადაცემის პროცესების მიმართ წაყენებულ მოთხოვნებს, კონკრეტულ ტექნოლოგიებსა და ინფორმაციაზე დაშვების უფლების მქონე პირების წრეს, ინფორმაციული ტექნოლოგიების უსაფრთხოდ და ეფექტურად გამოყენებისთვის აუცილებელ მოთხოვნებს, განსაზღრავს უნივერსიტეტის სტრუქტურული ერთეულების, აკადემიური/მოწვეული/დამხმარე პერსონალის (შემდეგში - პერსონალი) და სტუდენტების ვალდებულებებს, უნივერსიტეტის ინფორმაციულ ტექნოლოგიებთან და საინფორმაციო რესურსებთან წვდომის ნაწილში.

1.2. წინამდებარე პოლიტიკის მიზანია უნივერსიტეტის საგანმანათლებლო, ადმინისტრაციული და ბიზნეს პროცესების შეუფერხებელი მიმდინარეობის, უნივერსიტეტის ინფორმაციული ტექნოლოგიებისა და ინფორმაციული რესურსების გამართული ფუნქციონირების და ოპერირების ხელშეწყობა, ინფორმაციული უსაფრთხოების დაცვის უზრუნველყოფა, ინფორმაციული ტექნოლოგიებით უნივერსიტეტის საქმიანობის ეფექტურად და უსაფრთხოდ მხარდაჭერისთვის აუცილებელი პროცედურების დანერგვა.

1.3. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა მიმართულია უნივერსიტეტთან დაკავშირებული პირების (პერსონალი და სტუდენტები) კონფიდენციალურობისა და პერსონალური მონაცემების დაცვაზე.

1.4. პოლიტიკის მოთხოვნების შესრულება სავალდებულოა უნივერსიტეტის ინფორმაციულ ტექნოლოგიებზე წვდომის მქონე თითოეული მომხმარებლისთვის (პერსონალი და სტუდენტები).

1.5. პოლიტიკის მოთხოვნათა შეუსრულებლობა იწვევს ამ დოკუმენტით, უნივერსიტეტის შინაგანაწესით და სხვა სამართლებრივი აქტებით განსაზღვრულ პასუხისმგებლობას.

მუხლი 2. ინფორმაციული ტექნოლოგიების შეძენისა და ინსტალაციის პოლიტიკა

2.1. ინფორმაციული ტექნოლოგიებისა და შესაბამისი პროგრამული უზრუნველყოფის (hardware, software) შესყიდვა წარმოებს უნივერსიტეტის საქმიანობის სპეციფიკიდან და დადგენილი სამიზნე ნიშნულებიდან გამომდინარე.

2.2. ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენის საჭიროება შესაძლებელია გამომდინარეობდეს სტრუქტურული ერთეულის პერსონალის ან/და შესასრულებელი სამუშაოების სპექტრის გაზრდის, არსებული რესურსების ცვეთის/მწყობრიდან გამოსვლის/ახალ ამოცანებთან შეუსაბამობის, ან სხვა მიზეზით, რომელიც აღინიშნება შესაბამისი სტრუქტურული ერთეულის ხელმძღვანელის სამსახურებრივ ბარათში.

2.3. უნივერსიტეტის სტრატეგიული განვითარების გეგმით გათვალისწინებული ამოცანის შესრულებისთვის აუცილებელი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული

უზრუნველყოფის შეძენის მოთხოვნას წარადგენს უნივერსიტეტის სტრატეგიულ განვითარებაზე პასუხისმგებელი სტრუქტურული ერთეული/დასაქმებული.

2.4. უნივერსიტეტის კონკრეტული სტრუქტურული ერთეულის საჭიროებებს, ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენასთან დაკავშირებით, შესაბამისი სტრუქტურული ერთეულის ხელმძღვანელი წარუდგენს რექტორის მოადგილეს ადმინისტრაციული და საფინანსო მიმართულებით.

2.5. რექტორის მოადგილე ადმინისტრაციული და საფინანსო მიმართულებით იხილავს მოთხოვნას, ის უფლებამოსილია უარი თქვას ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენის მოთხოვნებზე იმ შემთხვევაში, თუ:

ა) უნივერსიტეტის სტრუქტურული ერთეულის მიერ არ არის დასაბუთებული შესაბამისი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის საჭიროება;

ბ) არსებობს ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის უკეთესი ალტერნატივა;

გ) ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენა შეუძლებელია შესაბამისი ბიუჯეტის არარსებობის გამო.

2.6. ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენაზე რექტორის მოადგილის უარი შესაძლებელია გასაჩივრდეს უნივერსიტეტის რექტორთან. რექტორი უფლებამოსილია მიიღოს გადაწყვეტილება დამატებითი ბიუჯეტის გამოყოფის შესახებ.

2.7. შესყიდვის მოთხოვნაზე დასტურის შემთხვევაში, რექტორის მოადგილე ადმინისტრაციული და საფინანსო მიმართულებით მოთხოვნას გადასცემს ინფორმაციული ტექნოლოგიების სამსახურს, რომელიც თავის მხრივ ვალდებულია, რექტორის მოადგილეს განსაზღვრულ ვადაში წარუდგინოს შემდეგი ინფორმაცია:

ა) დასკვნას მოთხოვნილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის სამუშაო ამოცანასთან რელევანტურობის, უნივერსიტეტში მოქმედ სხვა ტექნოლოგიებთან ინტეგრირების შესაძლებლობის, ბაზარზე ხელმისაწვდომობისა და უკეთესი ალტერნატივების არარსებობის შესახებ;

ბ) ინფორმაციას ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის მომწოდებელთა შესახებ (არანაკლებ 3 მომწოდებელი);

გ) ინფორმაციას თითოეულ მომწოდებელთან ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის ღირებულების შესახებ;

დ) ინფორმაციას დამატებითი მომსახურების - ტრანსპორტირება, განბაჟება, ინსტალაცია და სხვა საჭიროების შესახებ.

2.8. ინფორმაციული ტექნოლოგიების სამსახური უფლებამოსილია წარმოადგინოს 3-ზე ნაკლები მომწოდებელი იმ შემთხვევაში, თუ:

ა) მოთხოვნილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის ღირებულება არ აღემატება 300 ლარს;

ბ) მოთხოვნილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის შეძენა მისი მწარმოებელი კომპანიიდან ხდება (ლიცენზირებული ოპერაციული სისტემა ან პროგრამული უზრუნველყოფის პაკეტი, აპლიკაცია, სერვისი და სხვა).

2.9. რექტორის მოადგილე ადმინისტრაციული და საფინანსო მიმართულებით, ინფორმაციული ტექნოლოგიების სამსახურის ინფორმაციის საფუძველზე იღებს გადაწყვეტილებას მომწოდებლის არჩევისა და მასთან საქონლის/მომსახურების შესყიდვის ხელშეკრულების გაფორმების შესახებ.

2.10. შეძენილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის მონტაჟსა და ინსტალაციას ახორციელებს ინფორმაციული ტექნოლოგიების სამსახური, თუ მისი დასკვნით, არ არის აუცილებელი ინსტალაციის მომსახურების დამატებით შეძენა.

2.11. შეძენილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის ვარგისიანობის შემოწმება, მიღება-ჩაბარების აქტის გაფორმება და საჭიროების შემთხვევაში - საგარანტიო მომსახურების ან ხარვეზის აღმოფხვრის (Bugfixing) პროცესების ორგანიზება ეკისრება ინფორმაციული ტექნოლოგიების სამსახურს.

2.12. შეძენილი ინფორმაციული ტექნოლოგიებისა თუ პროგრამული უზრუნველყოფის მიღებას ადასტურებს შესაბამისი სტრუქტურული ერთეულის ხელმძღვანელი, რომელსაც გადაეცა შესაბამისი პროდუქტი.

მუხლი 3. მოწყობილობათა გამოყენების პოლიტიკა

3.1. უნივერსიტეტის თითოეული დასაქმებული აღჭურვილია მისი სამსახურებრივი მოვალეობის შესასრულებლად აუცილებელი ინფორმაციული ტექნოლოგიებით.

3.2. უნივერსიტეტში ადმინისტრაციულ/დამხმარე პოზიციაზე დასაქმებულს უნივერსიტეტი გამოუყოფს პერსონალურ კომპიუტერს, მისი სამსახურებრივი ფუნქციების ეფექტურად შესრულებისთვის აუცილებელი პროგრამული უზრუნველყოფით.

3.3. დასაქმებულის მიერ საკუთარი ინფორმაციული ტექნოლოგიების (ლეპტოპის, პლანშეტის, სმარტფონის და სხვა) გამოყენება დასაშვებია, მისი სტრუქტურული ერთეულის ხელმძღვანელის, ან ამ უკანასკნელის არარსებობის შემთხვევაში - ზემდგომი სტრუქტურული ერთეულის ხელმძღვანელის თანხმობით. თანხმობის გაცემისთვის, უფლებამოსილი პირი უნდა დარწმუნდეს რომ მსგავსი სახის ნებართვა არ წარმოშობს უნივერსიტეტის ინფორმაციის დაზიანების, დაკარგვის, ასევე, არაუფლებამოსილ პირთა მხრიდან მაზე წვდომის ან კიბერუსაფრთხოების დარღვევის რისკს.

3.4. დასაქმებულის მიერ უნივერსიტეტის ინფორმაციული ტექნოლოგიების უნივერსიტეტის კამპუსის (შენობის) გარეთ გამოყენება დასაშვებია, მისი სტრუქტურული ერთეულის ხელმძღვანელის და ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის თანხმობით. თანხმობის გაცემამდე, უფლებამოსილი პირები უნდა დარწმუნდნენ, რომ მსგავსი სახის ნებართვა არ წარმოშობს უნივერსიტეტის ტექნიკის ან/და მასზე არსებული ინფორმაციის დაზიანების, დაკარგვის, ასევე, არაუფლებამოსილ პირთა მხრიდან მაზე წვდომის ან კიბერუსაფრთხოების დარღვევის რისკს.

3.5. უნივერსიტეტის კომპიუტერულ ტექნიკაზე უნივერსიტეტის დასაქმებული მუშაობს მომხმარებლის (user) ანგარიშით. საკუთარი ინფორმაციული ტექნოლოგიების გამოყენების დროს, უნივერსიტეტის დასაქმებული ვალდებულია შექმნას მომხმარებლის ანგარიში, დაუშვებელია უნივერსიტეტის რესურსებთან მუშაობა ადმინისტრატორის (device administrator) უფლებით.

3.6. იმ ინფორმაციული ტექნოლოგიების გამოყენებისას, სადაც ადმინისტრატორის უფლების შეზღუდვა არ არის გათვალისწინებული (პლანშეტები, სმარტფონები) დასაქმებული იღებს ვალდებულებას არ დააინსტალიროს ნებისმიერი სახის პროგრამული უზრუნველყოფა აპლიკაციათა ოფიციალური მაღაზიის (Play Store, App Store) გვერდის ავლით ან/და არ მოახდინოს მოწყობილობის სუპერმომხმარებლის უფლების მოპოვება (Root, Jailbreak).

3.7. უნივერსიტეტის კომპიუტერული რესურსით, ასევე უნივერსიტეტის ინტერნეტ ქსელში მუშაობისას, უნივერსიტეტის დასაქმებულს ეკრძალება:

ა) ნებისმიერი პროგრამული უზრუნველყოფის ინსტალაცია;

ბ) მუშაობა ადმინისტრატორის უფლებით;

გ) ტექნიკის არამიზნობრივად გამოყენება;

დ) მოწყობილობათა ექსპლუატაციის წესის დარღვევა.

3.8. უნივერსიტეტის დასაქმებული უფლებამოსილია, ინფორმაციული ტექნოლოგიების სამსახურს მოთხოვოს უნივერსიტეტის საქმიანობისთვის გამოყენებული ინფორმაციული ტექნოლოგიების შემოწმება, მათში მავნე პროგრამული უზრუნველყოფის (malware) არარსებობის კუთხით. თავის მხრივ, ინფორმაციული ტექნოლოგიების სამსახური უფლებამოსილია დასაქმებულს მოსთხოვოს სამსახურეობრივი მიზნით გამოყენებად ტექნიკაზე ფუნქციონირებადი ანტივირუსული პროგრამის დაყენება.

3.9. უნივერსიტეტის მიერ შეძენილი პროგრამული უზრუნველყოფის ინსტალაცია პერსონალურ ინფორმაციულ ტექნოლოგიებზე დასაშვებია ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის ნებართვით და მის მიერ განსაზღვრული პერიოდით. დაუშვებელია უნივერსიტეტის დასაქმებულის სარგებლობაში გადაცემული უნივერსიტეტის მიერ შეძენილი პროგრამული უზრუნველყოფის სხვა მიზნით გამოყენება.

3.10. პორტატული მეხსიერების ბარათებით და დისკებით (USB, Flash, HDD, SDD) სარგებლობა დასაშვებია იმ შემთხვევაში, თუ ინფორმაციის გამცემ და ინფორმაციის მიმღებ კომპიუტერულ ტექნიკაზე გამართულია და ფუნქციონირებს ანტივირუსული პროგრამა. შესაბამისი ინფორმაციის არარსებობის შემთხვევაში, ინფორმაციის პორტატული მატარებელი ექვემდებარება ანტივირუსულ შემოწმებას ინფორმაციული ტექნოლოგიების სამსახურის მიმართ.

3.11. საერთო სარგებლობის ინფორმაციული ტექნოლოგიებისთვის (პრინტერი, სკანერი, სერვერი და სხვა) განისაზღვრება მის ეფექტურ ფუნქციონირებაზე პასუხისმგებელი დასაქმებული.

3.12. უნივერსიტეტის კომპიუტერული ტექნიკის მიღებით/ჩაბარებით დასაქმებულის ადასტურებს, რომ იცნობს შესაბამისი ტექნიკის ჩვეულებრივი, სამომხმარებლო დონეზე

გამოყენების წესებს და აღნიშნული ტექნიკით სარგებლობის პროცესში პასუხისმგებელია დადგენილი წესების დაცვაზე.

3.13. უნივერსიტეტის სხვა დასაქმებულის კომპიუტერული ტექნიკით სარგებლობა შესაძლებელია მისი მოსარგებლე დასაქმებულის, ან მისი არყოფნის შემთხვევაში - ამ დასაქმებულის ხელმძღვანელის ნებართვით.

3.14. მომხმარებლის მიერ ტექნიკის არასწორი მოხმარებით, განზრახ, ან აღნიშნული პოლიტიკით დადგენილი მოთხოვნების დაუცველობით გამოწვეული დაზიანებით დამდგარ ზარალზე პასუხისმგებელია შესაბამისი ტექნიკის მომხმარებელი თანამშრომელი. აღნიშნული არ მოიცავს ტექნიკის ბუნებრივი ცვეთის, სხვა მიზეზით მწყობრიდან გამოსვლის, ასევე პერიფერიული მოწყობილობების და გაყვანილობის ჩვეულებრივი მოხმარების პროცესში დაზიანების შემთხვევებს.

3.15. ტექნიკის დაზიანების შემთხვევაში, აღნიშნული ტექნიკა უნდა გადაეცეს ინფორმაციული ტექნოლოგიების სამსახურს, რომელიც ადგენს დაზიანების გამომწვევ მიზეზებსა და უზრუნველყოფს მის შეკეთებას წინამდებარე წესის მე-2 მუხლით დადგენილი პროცედურით, ან მიმართავს ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილეს, ტექნიკის ჩამოწერის თაობაზე.

3.16. დასაქმებულის საკუთრებაში არსებული მოწყობილობის დაზიანების შემთხვევაში, რომელიც შეიცავდა უნივერსიტეტისთვის ღირებულ ინფორმაციას, დასაქმებული ვალდებულია აღნიშნულთან დაკავშირებით ინფორმაცია შეატყობინოს საკუთარ ხელმძღვანელსა და ინფორმაციული ტექნოლოგიების სამსახურს და გადასცეს მოწყობილობა, უნივერსიტეტის ინფორმაციის ამოღების მიზნით. უნივერსიტეტისთვის ღირებული ინფორმაციის დაკარგვის რისკის არსებობის შემთხვევაში, ხელმძღვანელის ნებართვის გარეშე დასაქმებული არ არის უფლებამოსილი შეაკეთოს ან მოახდინოს მოწყობილობის უტილიზაცია.

3.17. ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის კოორდინირებით ხორციელდება უნივერსიტეტის კომპიუტერული აღჭურვილობებისა და სხვა ინფორმაციული მოწყობილობების ინვენტარიზაცია, მათი ტექნიკური გამართულობის აუდიტი.

3.18. დასაქმებულთან შრომითი ურთიერთობის შეწყვეტის შემთხვევაში, დასაქმებული ვალდებული ჩააბაროს ინფორმაციული ტექნოლოგიების სამსახურს მასზე გადაცემული ტექნიკა, ასევე მის საკუთრებაში არსებული მოწყობილობიდან ამოიღოს და ინფორმაციული ტექნოლოგიების სამსახურს გადასცეს უნივერსიტეტის საქმიანობასთან დაკავშირებული ინფორმაცია.

მუხლი 4. ელექტრონული ფოსტის გამოყენების პოლიტიკა

4.1. უნივერსიტეტის პერსონალის წარმომადგენლები თავიანთი პროფესიული საქმიანობის განხორციელებისას, ვალდებულნი არიან გამოიყენონ უნივერსიტეტის დომეინურ სახელზე (...@avicenna.ge) შექმნილი ელექტრონული ფოსტა.

4.2. უნივერსიტეტის სტუდენტები, უნივერსიტეტთან კომუნიკაციას, ასევე სასწავლო პროცესის მართვის სისტემაში ავტორიზაციას უზრუნველყოფენ უნივერსიტეტის დომეინურ სახელზე (...**@avicenna.ge**) შექმნილი ელექტრონული ფოსტის მისამართის გამოყენებით.

4.3. ელექტრონული ფოსტის მისამართი უნივერსიტეტის დომენზე იქმნება ინფორმაციული ტექნოლოგიების სამსახურის მიერ და უნივერსიტეტში დასაქმებულს/სტუდენტს გადაეცემა დროებითი ავტორიზაციის (temporary login) მონაცემებით, რომელიც ექვემდებარება სავალდებულო შეცვლას მომხმარებელი თანამშრომლის/**სტუდენტის** მიერ. მომხმარებლის მიერ გამოყენებული პაროლი უნდა იყოს მინიმუმ 8 სიმბოლოიანი, შეიცავდეს რომაულ ასოებს, არაბულ ციფრებსა და დამატებით სიმბოლოებს. დაუშვებელია პაროლში მომხმარებლის სახელის, გვარის, დაბადების წელის და უნივერსიტეტის დასახელების გამოყენება (რეკომენდირებულია მრავალფაქტორიანი, მინიმუმ 2 საფეხურიანი აუთენტიფიკაციის სისტემის გამოყენება).

4.4. ელექტრონული ფოსტის მომხმარებლის სახელი ადმინისტრაციისა და აკადემიური, მოწვეული და სამეცნიერო პერსონალის შემთხვევაში იქმნება ლათინურ ტრანსკრიპციაში მისი სახელის პირველი ასოს (ინიციალი) და მისი გვარის კომბინაციით: N.Surname@avicenna.ge , ხოლო სტუდენტის შემთხვევაში - ლათინურ ტრანსკრიპციაში მისი სახელისა და გვარის კომბინაციით: Name.Surname@avicenna.ge. იდენტური სახელებისა და გვარების შემთხვევაში, დასაშვებია მომხმარებლის სახელში დამატებით არაბული ციფრების გამოყენება: N.Surname@avicenna.ge / Name.Surname1@avicenna.ge.

4.5. ადმინისტრაციის, აკადემიური და მოწვეული პერსონალის ელექტრონული ფოსტის ანგარიშებზე, სავალდებულოა საზოგადოებასთან ურთიერთობისა და მარკეტინგის სამსახურის მიერ მოწოდებული ხელმოწერის ფორმის გამოყენება, უნივერსიტეტის სიმბოლიკის, დასაქმებულის მიერ დაკავებული თანამდებობის/პოზიციისა და საკონტაქტო ინფორმაციის მითითებით.

4.6. დაუშვებელია ელექტრონული ფოსტის არასამსახურეობრივი მიმოწერისთვის გამოყენება.

4.7. დაუშვებელია არასამსახურეობრივი მიზნით ელექტრონული ფოსტის მისამართის რეგისტრირება სხვადასხვა რესურსებზე, მათ შორის ელექტრონული კომერციის პლატფორმებზე, გარდა შესყიდვებზე პასუხისმგებელი სტრუქტურული ერთეულებისა და სოციალურ ქსელებში - გარდა საზოგადოებრივი ურთიერთობებისა და მარკეტინგის სამსახურისა და სხვა.

4.8. დაუშვებელია ელექტრონული ფოსტის ანგარიშის დაუცველად დატოვება, ანგარიშიდან გასვლის (log out) ან მომხმარებლის ანგარიშის კომპიუტერზე დახურვის (lock) გარეშე.

4.9. სხვა მოწყობილობებზე ელექტრონული ფოსტით სარგებლობისას აუცილებელია ბრაუზერში „Incognito“ რეჟიმის ჩართვა, ხოლო სესიის დასრულების შემდეგ - ანგარიშიდან გამოსვლა (Sign out).

4.10. ელექტრონული ფოსტით სარგებლობის უსაფრთხოების წესები ელექტრონულ ფოსტასთან ერთად თანაბარწილად ვრცელდება „GSuite“ პაკეტში შემავალი სხვა ვებაპლიკაციების (sheets, forms, docs და სხვა) გამოყენებაზე.

4.11. კორპორატიული ელექტრონული ფოტის მომხმარებელი ვალდებულია შეასრულოს მომსახურების პროვაიდერის (Google) სერვისის პირობები.

4.12. უნივერსიტეტი უფლებამოსილია გააკონტროლოს მომხმარებლის მიერ კორპორატიული ელექტრონული ფოსტის გამოყენება და დამატებითი ნებართვის გარეშე მოიპოვოს წვდომა, შეცვალოს ან გააუქმოს მომხმარებლის ანგარიში.

4.13. მომხმარებლის ანგარიშიდან შესრულებული თითოეული ოპერაცია მიიჩნევა მომხმარებლის მიერ შესრულებულად.

4.14. ელექტრონული ფოსტის ანგარიშზე წვდომის დაკარგვის, ან ანგარიშით სარგებლობის ნებისმიერი სხვა დაბრკოლების შექმნის შემთხვევაში, მომხმარებელი ვალდებულია ამის შესახებ დაუყოვნებლივ შეატყობინოს ინფორმაციული ტექნოლოგიების სამსახურს.

მუხლი 5. სოციალური მედიის გამოყენების პოლიტიკა

5.1. სოციალური მედიის გამოყენება დასაშვებია:

ა) სამსახურებრივი მიზნებისთვის - როგორც ინფორმაციის მოძიების, ასახვის და გავრცელების პლატფორმა;

ბ) პირადი მიმოწერისთვის - სოც. მედიის პლატფორმებზე არსებული მესენჯერების ფუნქციონალის ფარგლებში;

გ) სხვა პირადი მიზნებისთვის - თუ აღნიშნული ხელს არ უშლის დასაქმებულის მიერ სამსახურებრივი ფუნქციების შესრულებას.

5.2. უნივერსიტეტის სოციალური მედია არხებზე წვდომასა და კონტროლს ახორციელებს უნივერსიტეტის საზოგადოებასთან ურთიერთობისა და მარკეტინგის სამსახური.

5.3. დაუშვებელია უნივერსიტეტის სახელით ანგარიშის შექმნა ან/და მისი ვერიფიცირების მცდელობა ნებისმიერ სოციალურ ქსელსა და სოციალური მედიის სხვა პლატფორმაზე (ბლოგი, ვლოგი, მიკრობლოგი და სხვა) ან უნივერსიტეტის სახელით საკუთარ სოციალურ მედია არხებზე კომუნიკაცია.

5.4. უნივერსიტეტის დასაქმებულს უფლება აქვს სოციალური მედიის პირად გვერდზე განათავსოს რელევანტური ინფორმაცია დამსაქმებლის, მისი სამუშაო პოზიციისა და გამოცდილების შესახებ.

5.5. უნივერსიტეტის, მისი პერსონალის, სტუდენტების, პარტნიორების და უნივერსიტეტთან დაკავშირებული პირების შესახებ სოციალურ მედიაში ინფორმაციის გავრცელება უნდა განხორციელდეს პერსონალური მონაცემების დაცვის შესახებ საქართველოს კანონმდებლობის და უნივერსიტეტის ეთიკის კოდექსით დადგენილი მოთხოვნების დაცვით, ობიექტური და კოლეგიალური ფორმით.

5.6. უნივერსიტეტის სოციალური მედიის გვერდებზე აკრძალულია სპამი (კონტექსტთან შეუსაბამო ინფორმაციის მოწოდება), ღია თუ ფარული რეკლამა, პოლიტიკური პროპაგანდა, სიძულვილისა და დისკრიმინაციის ენის გამოხატვა.

5.7. უნივერსიტეტი უფლებამოსილია შეაფასოს სოციალურ მედიაში დასაქმებულის მიერ უნივერსიტეტსა თუ კოლეგის მიმართ გამოთქმული მოსაზრება, უნივერსიტეტის შინაგანაწესთან და ეთიკური ქცევის სტანდარტთან შესაბამისობაზე, გამოხატვის თავისუფლების პრინციპის აღიარებით.

მუხლი 6. ინტერნეტის გამოყენების პოლიტიკა

6.1. უნივერსიტეტის ტერიტორიაზე ინტერნეტის გამოყენება დასაშვებია უნივერსიტეტის კაბელიანი ან უკაბელო ქსელის გამოყენებით.

6.2. უნივერსიტეტის ადმინისტრაციის ყველა დასაქმებულს ეძლევა ქსელში შესასვლელი პაროლი.

6.3. სტუდენტებისთვის ფუნქციონირებს სტუმრისთვის გამოყოფილი (უპაროლო) ქსელი.

6.4. დაუშვებელია სამსახურებრივი მიზნებისთვის სტუმრის (Guest) ქსელთან დაკავშირება.

6.5. უნივერსიტეტს გარეთ ინტერნეტ ქსელთან დაკავშირებისას მომხმარებელმა უნდა დაიცვას ქსელური უსაფრთხოების შემდეგი პროცედურები:

ა) იქონიოს უნივერსიტეტის ინფორმაციული ტექნოლოგიების სამსახურის მიერ რეკომენდირებული, აქტუალურ ვერსიამდე განახლებული ანტივირუსული პროგრამა;

ბ) არ გადავიდეს შეუმოწმებელ, საეჭვო (phishing) ბმულებზე;

გ) არ განახორციელოს ფინანსური, პერსონალური მონაცემების და უნივერსიტეტის ინტელექტუალურ საკუთრებას მიკუთვნებულ ინფორმაციასთან მუშაობა, სათანადო დაცვის (https სერტიფიკატის) არმქონე ვებგვერდებზე.

6.6. ინტერნეტის გამოყენება უნივერსიტეტში სამუშაო პროცესში დასაშვებია, ამ მუხლით გათვალისწინებული შეზღუდვების გათვალისწინებით.

6.7. აკრძალულია VPN და P2P კავშირის გამოყენება, IP მისამართის შეცვლა, ასევე უნივერსიტეტის ინფორმაციული ტექნოლოგიების სამსახურის მიერ არარეკომენდირებული ბრაუზერით (Internet Explorer, ToR და სხვა) სარგებლობა.

6.8. მომხმარებლის ბრაუზერი განახლებული უნდა იყოს უახლეს აქტუალურ ვერსიამდე.

6.9. პირადი მიზნებისთვის ინტერნეტ კავშირის, მათ შორის, საინფორმაციო წყაროების, სოციალური ქსელების, პერსონალური ელექტრონული ფოსტის გამოყენება დასაშვებია გონივრულ ფარგლებში, თუ აღნიშნული ხელს არ უშლის დასაქმებულის მიერ სამსახურებრივი ფუნქციების შესრულებას. დასაქმებულის უშუალო ხელმძღვანელი უფლებამოსილია მოსთხოვოს დასაქმებულს შეწყვიტოს ინტერნეტ რესურსებით საკუთარი მიზნებისთვის სარგებლობა.

6.10. აკრძალულია ინტერნეტში პორნოგრაფიული, ძალადობისა და სიძულვილის ენის შემცველი რესურსებით, ასევე ვებ ინტერფეისის მქონე კომპიუტერული თამაშებით სარგებლობა.

6.11. აკრძალულია .exe გაფართოების მქონე ფაილების ჩამოტვირთვა და მათი ინსტალაციის მცდელობა.

6.12. უნივერსიტეტი უფლებამოსილია დაადგინოს აკრძალული ვებგვერდების სია და შეზღუდოს მათზე მომხმარებელთა წვდომა.

6.13. უნივერსიტეტის ინფორმაციული ტექნოლოგიების სამსახური უფლებამოსილია გააკონტროლოს მომხმარებლის „ტრაფიკი“ და წარუდგინოს ადმინისტრაციულ და საფინანსო მიმართულებით რექტორის მოადგილეს ინფორმაცია მომხმარებლის ვებ-ისტორიის შესახებ.

მუხლი 7. ანგარიშების მართვა

7.1. უნივერსიტეტში ფუნქციონირებს ინფორმაციული ტექნოლოგიების მომხმარებლების ანგარიშების შემდეგი ჯგუფები:

ა) ადმინისტრატორი და ოპერატორი - ინფორმაციული ტექნოლოგიების მართვის სამსახური;

ბ) სპეციალური უფლების მქონე მომხმარებელი - განისაზღვრება ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის მიერ;

გ) ჩვეულებრივი მომხმარებელი - უნივერსიტეტის ყველა დასაქმებული, თუ მას რექტორის მოადგილის გადაწყვეტილებით არ აქვს მინიჭებული სპეციალური უფლება;

დ) სტუდენტი - სტუდენტი მომხმარებელი.

7.2. მომხმარებელთა ჯგუფები სარგებლობენ მათთვის გამოყოფილი ფიზიკური თუ ელექტრონული მოწყობილობებითა და სერვისებით. სპეციფიკიდან გამომდინარე არსებობს ჯგუფის შიდა დამატებითი წვდომის დონეები.

7.3. მომხმარებლების ჯგუფებისა და დონეების განსაზღვრა/ცვლილება ხდება წინასწარ, ინფორმაციული ტექნოლოგიების სამსახურის მიერ, ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილესთან შეთანხმებით.

7.4. მომხმარებელთა ანგარიშების შექმნის, შეცვლის, აქტივობის მონიტორინგისა და გაუქმების უფლებამოსილება ენიჭება სისტემურ ადმინისტრატორს.

7.5. მომხმარებლების ჯგუფებისა და დონეების შეუსაბამო ქმედება გამოიწვევს:

ა) მოწყობილობებთან და ელექტრონულ სერვისებთან წვდომის შეზღუდვას;

ბ) საუნივერსიტეტო ქსელიდან განცალკევებას ან/და იზოლირებას.

7.6. ადმინისტრატორი ან სპეციალური უფლების მქონე მომხმარებელი, უფლებამოსილია კონკრეტული ამოცანის შესასრულებლად ან პრობლემის გადასაჭრელად, მომხმარებლის თანხმობით, მის ანგარიშზე მოიპოვოს დისტანციური წვდომა (remote access).

7.7. დაშვების წერტილების ფუნქციური ჯგუფები და მართვა:

7.7.1. უნივერსიტეტის შიდა სტრუქტურიდან გამომდინარე, ყველა ჯგუფისთვის გამოყოფილია დამოუკიდებელი შიდა ქსელი (ფიზიკური ან/და ვირტუალური) და ასრულებს კონკრეტული ჯგუფის მოთხოვნებს უსაფრთხოების და ხელმისაწვდომობის კუთხით;

7.7.2. ჯგუფი განკუთვნილია შიდა საუნივერსიტეტო ქსელის, მოწყობილობებისა და სერვისების მართვისთვის. აქვს წვდომა ყველა სხვა ჯგუფთან და აგრეთვე გამოყოფილ სერვისებთან და მოწყობილობებთან. ჯგუფთან წვდომა აქვს მხოლოდ ქსელის/სისტემურ ადმინისტრატორს და ოპერატორებს, ამასთან ოპერატორებს აქვთ შეზღუდული უფლებები (მხოლოდ წვდომა შეცვლის უფლების გარეშე).

ა) დასაქმებულთა ჯგუფი - ჯგუფი განკუთვნილია უნივერსიტეტის დასაქმებულთათვის და დაშვებულია მოწყობილობებს შორის ინფორმაციის ურთიერთგაცვლა. შეზღუდულია სხვა ჯგუფებთან კომუნიკაცია;

ბ) სტუმრებისა და სტუდენტების ჯგუფი - ჯგუფი განკუთვნილია სტუმრებისთვის და სტუდენტებისთვის და დაშვება აქვს მხოლოდ განსაზღვრულ ინტერნეტ სერვისებთან, შეზღუდული დროით;

გ) უსაფრთხოებისა და ტელეფონიის ჯგუფი - ჯგუფი განკუთვნილია სამეთვალყურეო კამერების, ტელეფონის და მათი სამართავი მოწყობილობებისთვის. შეზღუდულია მესამე პირისა და მოწყობილობების თვითნებური წვდომა ჯგუფთან. ამ ქსელთან დაშვება აქვთ მხოლოდ რეგისტრირებულ მოწყობილობებს. ასევე, შეზღუდულია წვდომა სხვა ჯგუფებთან და ცალკეულ სერვისებთან.

დ) საგამოცდო და ლაბორატორიული ჯგუფი - ჯგუფი განკუთვნილია ელექტრონული გამოცდებისა და ლაბორატორიული საქმიანობისთვის. დაშვებულის მხოლოდ საგამოცდო და ლაბორატორიულ რესურსთან წვდომა. შეზღუდულია სხვა ჯგუფებთან და ცალკეულ სერვისებთან წვდომა.

ე) სატელეკომუნიკაციო კვანძებთან წვდომა - სატელეკომუნიკაციო კვანძებთან წვდომის უფლება აქვს მხოლოდ ადმინისტრატორს და ოპერატორს. უსაფრთხოების მიზნით, დაკეტილია როგორც სატელეკომუნიკაციო შახტა. აპარატურასთან წვდომისთვის საჭიროა:

ე.1) დაშვების მიზნის და საჭიროების შესახებ ადმინისტრაციისთვის წერილობითი ინფორმირება (შეტყობინების/მიმართვის გაგზავნა);

ე.2) უსაფრთხოების სამსახურის შეტყობინება სატელეკომუნიკაციო შახტასთან წვდომისთვის;

ე.3) სამუშაოს დასრულების შემდეგ ოპერატორის და უსაფრთხოების სამსახურის შეტყობინება.

მუხლი 8. ინფორმაციული უსაფრთხოება

8.1. უნივერსიტეტში ინფორმაციული უსაფრთხოების პოლიტიკა ხორციელდება ფიზიკური, ქსელური და კიბერუსაფრთხოების დონეებზე:

ა) ფიზიკური უსაფრთხოება მოიცავს ანგარიშების, ვებ-აპლიკაციების და პროგრამული უზრუნველყოფის დაცვას პაროლით, ასევე სისტემური ადმინისტრირების ფუნქციების შეზღუდვას ჩვეულებრივი მომხმარებლებისთვის.

ბ) ქსელური უსაფრთხოება გულისხმობს ტექნიკური და პროგრამული უზრუნველყოფის (Switch, Firewall) გამოყენებას უნივერსიტეტის ფიზიკურ და უსადენო ქსელებზე არაავტორიზებული წვდომისგან დასაცავად.

გ) კიბერუსაფრთხოება მოიცავს ამ პოლიტიკის განსაზღვრულ შეზღუდვებს ინფორმაციის მატარებლების გამოყენების, მონაცემების შენახვის (Data Backup), აპლიკაციების ინსტალირების უფლების შეზღუდვის, ანგარიშების და პაროლების მართვის და მულტიფაქტორული აუთენტიფიკაციის მეთოდებს, რომელიც ამცირებს პროგრამული ან სოციალური ინჟინერიის გამოყენებით კიბერშეტევის რისკს.

8.2. რექტორის შესაბამისი ბრძანებით განსაზღვრული პირ(ებ)ის (ადმინისტრატორი და ოპერატორი) გარდა, არავის არ აქვს უფლება უნივერსიტეტის ქსელს თვითნებურად დაუკავშიროს მოწყობილობა, ხელოვნურად გააფართოვოს მისი დაფარვის არეალი ან განახორციელოს ნებისმიერი სხვა საქმიანობა, რომელიც არღვევს საუნივერსიტეტო ქსელის, სერვისებისა და მოწყობილობების საიმედოობას, უსაფრთხოებას, მთლიანობას და ხელმისაწვდომობას.

მუხლი 9. სასწავლო პროცესის მართვის სისტემის გამოყენების პოლიტიკა

9.1. უნივერსიტეტს სასწავლო პროცესის ელექტრონული სერვისების მართვის სისტემის მომსახურებას უწევს Outsource კომპანია.

9.2. სასწავლო პროცესის მართვის ელექტრონული სისტემის უსაფრთხოებაზე პასუხისმგებელია Outsource კომპანია, რაც რეგულირდება კომპანიასთან გაფორმებული მომსახურების ხელშეკრულებით.

9.3. უნივერსიტეტის სასწავლო პროცესის მართვის სისტემა (შემდეგში - სისტემა) - staff.avicenna.ge და students.avicenna.ge - უზრუნველყოფს უნივერსიტეტის საგანმანათლებლო და ადმინისტრაციულ საქმიანობის ეფექტურ წარმართვას, არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.

9.4. სისტემის ზოგადი ფუნქციებია (მოდულებია):

ა) უნივერსიტეტში სასწავლო პროცესის მართვის ავტომატიზაცია;

ბ) ფინანსური მოდულის ავტომატიზაცია (სახელფასო სქემისა და სწავლის საფასურის გადახდასთან/აღრიცხვასთან დაკავშირებული მოდული);

გ) ელექტრონული საქმისწარმოება;

დ) ადამიანური რესურსების მართვა (HR);

ე) ელექტრონული ბიბლიოთეკა;

ვ) ელექტრონული ტესტირება.

ზ) გამოკითხვები;

თ) რეპორტინგი;

ი) SMS შეტყობინებების გაგზავნა;

კ) ადმინისტრაციის/აკადემიური/მოწვეული პერსონალის ინდივიდუალური პანელი;

ნ) კომუნიკაცია ადმინისტრაციას, ლექტორებსა და სტუდენტებს შორის;

ნ) მომხმარებლის უფლებების განსაზღვრა;

ო) დღეში 3-ჯერ მონაცემების რეზერვაცია;

9.5. სისტემაში გამოყენებულია კრიპტოგრაფია, სადაც დაშიფრულია მომხმარებლების (ადმინისტრაცია, ლექტორი, სტუდენტი) პაროლები.

9.6. სისტემის მომხმარებლები არიან:

ა) ადმინისტრაცია;

ბ) ლექტორი;

გ) სტუდენტი.

9.7. სისტემის უსაფრთხოება:

9.7.1. სისტემის კოდი იწერება სპეციალურად გამოყოფილ ლოკალურ სერვერზე, სადაც ხდება სისტემაში დამატებული ახალი მოდულის ტესტირება, შემდეგ ხდება შემოწმებული კოდის ატვირთვა ძირითად სერვერზე;

9.7.2. სისტემა მუშაობს GDPR (General Data Protection Regulation) სტანდარტზე, სერვერზე ინახება მოქმედებათა ლოგები, შემდეგი მონაცემებით: მოქმედების ავტორი, მოქმედების დრო, შესრულებული მოქმედება, IP მისამართი;

9.7.3. ბიზნესის უწყვეტობის მიზნით, ძირითადი სერვერის მწყობრიდან გამოსვლის შემთხვევაში, ავტომატურად ირთვება სარეზერვო სერვერი, რომელიც ახდენს ძირითად სერვერთან რეპლიკაციას;

9.7.4. სისტემა განთავსებულია Google Cloud-ზე;

9.7.5. სისტემის მონაცემები დღეში 3-ჯერ ავტომატურად ინახება უნივერსიტეტის google drive-ზე;

9.8. სისტემის განვითარების მექანიზმები:

9.8.1. უნივერსიტეტში არსებული ქსელის ინფრასტრუქტურა მოწყობილია თანამედროვე სტანდარტებით. სტანდარტების ცვლილების შემთხვევაში, უნივერსიტეტი მუდმივად ზრუნავს ახალ სტანდარტებთან შესაბამისობაში მოიყვანოს თავისი ინფრასტრუქტურა.

9.8.2. არსებული სასწავლო პროცესის მართვის სისტემის კოდი იწერება არსებული სტანდარტებით, სტანდარტების ცვლილებასთან ერთად იცვლება პროგრამული უზრუნველყოფის მიდგომა და მისი გადაჭრის გზები.

9.8.3. უნივერსიტეტი უზრუნველყოფს საინფორმაციო რესურსების განვითარებას, გაუმჯობესებას, პროცესების ოპტიმიზაციასა და მონიტორინგს, როგორც ადმინისტრაციის პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუთსორსინგით.

მუხლი 10. დაშვების წერტილები და ინფორმაციული ტექნოლოგიები

10.1. უნივერსიტეტის საინფორმაციო ტექნოლოგიების და სატელეკომუნიკაციო ინფრასტრუქტურის დაგეგმარება და ინსტალაცია/მონტაჟი მოხდა საუნივერსიტეტო შენობის მშენებლობასთან ერთად და მაქსიმალურად გათვლილია უახლოესი 8-10 წლის განმავლობაში ტექნოლოგიების განვითარებასთან ადაპტირებისთვის.

10.2. უნივერსიტეტის ინფრასტრუქტურის ნაწილს წარმოადგენს, როგორც უნივერსიტეტის ტერიტორიაზე არსებული საუნივერსიტეტო ქსელი და მოწყობილობები, აგრეთვე სერვისები და მოწყობილობები, რომლებიც განთავსებულია ღრუბელში (Cloud) და სხვადასხვა დატაცენტრებში.

10.3. უნივერსიტეტის შენობის ტერიტორიაზე ყველა ოთახში განთავსებულია ფიზიკური დაშვების წერტილები, შესაძლებელია რადიოსიხშირული სპექტრით სარგებლობა.

10.4. უნივერისტეტის ტერიტორიაზე დანერგილია უახლესი, უსადენო მაღალი გამტარობის რადიო სიხშირული ქსელი, რომელიც იყენებს 802.3 a/b/g/n/ac სტანდარტს და მომხმარებლების ავტომატური როუმინგის ტექნოლოგიას. გამოიყენება WPA2 (სტანდარტი: IEEE 802.11i) პროტოკოლი AES შიფრაციის ალგორითმით.

10.5. უნივერისტეტის ტერიტორიაზე განთავსებული სადენიანი დაშვების წერტილები იყენებენ 1000BASE-T ტექნოლოგიას (სტანდარტი: 802.3ab-1999 (40)) და ფიზიკური გაყვანილობა, საჭიროების შემთხვევაში 2.5GBASE-T (სტანდარტი: 802.3bz-2016 (125)) ტექნოლოგიის გამოყენების საშუალებას იძლევა.

10.6. ვირტუალური შიდა ქსელისთვის გამოიყენება L2TP/IPSec , IPSec პროტოკოლები AES, DES, HMAC-SHA1/SHA2 შიფრაციის ალგორითმებით.

10.7. ქსელთან დაშვების უსაფრთხოების დონეები განისაზღვრება დაშვების ფუნქციური ჯგუფებისთვის წინამდებარე პოლიტიკის მიხედვით. ჯგუფებს აქვთ წვდომა მხოლოდ მათთვის განსაზღვრულ რესურსთან (ფიზიკურ და ელექტრონულ).

10.8. უნივერსიტეტის მთელ ტერიტორიაზე, აუდიტორიების და ადმინისტრაციის ოთახების გარდა, განთავსებულია ვიდეო სამეთვალყურეო სისტემა, რომელიც მოიცავს როგორც შენობის შიდა სივრცეს, აგრეთვე პერიმეტრს.

10.9. სამეთვალყურეო ქსელი წარმოადგენს დახურულ სისტემას, რომელთან წვდომა ცვლილება/ჩაწერის რეჟიმში იზღუდება ყველასთვის, ხოლო წაკითხვის რეჟიმში ხელმისაწვდომია მხოლოდ უსაფრთხოებაზე პასუხისმგებელი სტრუქტურული ერთეულისთვის.

10.10. სამეთვალყურეო სისტემაში განხორციელებული ნებისმიერი ქმედება ინახება ქსელურ ვიდეო ჩამწერში არსებულ ელექტრონული აღრიცხვის ჟურნალში.

10.11. უნივერსიტეტის ტერიტორიაზე დანერგილია VoIP ტექნოლოგიაზე დაფუძნებული ტელეფონიის სისტემა, რომელიც უზრუნველყოფს თანამშრომელთა ერთმანეთთან და აგრეთვე საქართველოს ტერიტორიაზე არსებულ სხვადასხვა სახაზო სატელეფონო ოპერატორების აბონენტებთან შეუფერხებელ კომუნიკაციას.

10.12. ყველა სატელეფონო მოწყობილობა წინასწარ რეგისტრირდება შიდა სატელეფონო სადგურზე და ენიჭება უნიკალური კოდი. დანიშნულების შესაბამისად, იზღუდება მოწყობილობის წვდომა სერვისებთან. საჭიროების შემთხვევაში გამოიყენება SRTP და TLS შიფრაციის ტექნოლოგიები.

10.13. ბიზნეს უწყვეტობის უზრუნველსაყოფად უნივერსიტეტში დანერგილია სხვადასხვა სარეზერვო სისტემა (ფიზიკური და ელექტრონული). უნივერსიტეტს აქვს „სთორეიჯ სერვერი“ (storage server). სერვერზე განთავსებული დოკუმენტების უსაფრთხოების უზრუნველსაყოფად, ყოველი დღის ბოლოს, სერვერზე ავტომატურად კეთდება ფაილების რეზერვი (Beckup) Google Drive-ზე.

10.14. უნივერსიტეტს ემსახურება ორი ინტერნეტ პროვაიდერი. სილქნეტი და მაგთიკომი. ძირითად ინტერნეტის წყაროდ გამოყენებულია სილქნეტის ხაზი. მაგთიკომის ხაზი კი გამოიყენება, როგორც რეზერვი წყარო.

10.15. ელექტრო ენერგიის უწყვეტი მიწოდებისთვის უნივერსიტეტს გააჩნია 500 კილოვატიანი დიზელის გენერატორი, რომელიც დენის წასვლიდან 3 წამში ირთვება ავტომატურად, ასევე უნივერსიტეტის პერსონალი აღჭურვილია დენის სარეზერვო სისტემით (UPS).

მუხლი 11. ინფორმაციული ტექნოლოგიების რესურსების მართვა

11.1. უნივერსიტეტის ინფორმაციული ტექნოლოგიების სამსახური პასუხისმგებელია ინფორმაციული სისტემებისა და სერვისების, ელექტრონული მონაცემთა ბაზებისა და ინფორმაციული ტექნოლოგიების გამართული ფუნქციონირების ადმინისტრირებაზე.

11.2. ინფორმაციული ტექნოლოგიების სამსახური:

ა) შეიმუშავებს უნივერსიტეტის ინფორმაციული ტექნოლოგიების, ინფორმაციული უსაფრთხოებისა და მონაცემთა დაცვის პროცედურებს;

ბ) კოორდინაციას უწევს უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონული სისტემის ფუნქციონირებას;

გ) ახდენს მონაცემთა ბაზების ადმინისტრირებას;

დ) პასუხისმგებელია უნივერსიტეტის კომპიუტერული აღჭურვილობების, ქსელის, სერვერის გამართულ ფუნქციონირებაზე;

ე) ახდენს უნივერსიტეტის ვებგვერდის ადმინისტრირებას;

ვ) ზედამხედველობს უნივერსიტეტში ინფორმაციული ტექნოლოგიების უსაფრთხოდ, დადგენილი პროცედურების შესაბამისად გამოყენებას;

ზ) მონაწილეობს ინფორმაციული ტექნოლოგიების შერჩევის, შესყიდვის, გამართვისა და შეფასების პროცესებში;

თ) ახორციელებს პერსონალის ინსტრუქტაჟს ინფორმაციული ტექნოლოგიების ეფექტურად და უსაფრთხოდ გამოყენებასთან დაკავშირებით;

ი) თავისი კომპეტენციის ფარგლებში, ზრუნავს ინოვაციური ტექნოლოგიების უნივერსიტეტის საგანმანათლებლო და ადმინისტრირების პროცესში იმპლემენტაციაზე;

კ) ახორციელებს უნივერსიტეტის სამართლებრივი აქტებით განსაზღვრულ სხვა უფლებამოსილებებს.

11.3. ინფორმაციული ტექნოლოგიების სამსახური ვალდებულია:

ა) მომხმარებლები უზრუნველყოს ჯგუფისთვის წინასწარ განსაზღვრული რესურსებით, გააცნოს მათი ექპლუატაციის წესები, დარღვევის შემთხვევაში დროებით შეუჩეროს ან შეუწყვიტოს რესურსთან წვდომა;

ბ) ტექნოლოგიების, სტანდარტებისა და სერვისების სამომავლო განვითარება და ცვლილებასთან ერთად, შეიმუშავოს, დანერგოს და მართოს ახალი ინფორმაციული ტექნოლოგიების რესურსები. ახალი სერვისის, მოწყობილობის, ქსელის და ტექნოლოგიის დანერგვა ან/და არსებულის ცვლილება უნდა შეესაბამებოდეს უნივერსიტეტის სტრატეგიული განვითარებისა და ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას;

გ) განახორციელოს საუნივერსიტეტო ელექტრონული თუ ფიზიკური ქსელის, სერვისებისა და მოწყობილობების მონიტორინგი. ნებისმიერი ხარვეზის აღმოჩენის შემთხვევაში დაუყოვნებლივ აღმოფხვრას იგი. ქსელიდან განაცალკევოს ან იზოლირება მოახდინოს მოწყობილობების ან სერვისების რომლებიც ხელს უშლის ან/და საფრთხეს უქმნის საუნივერსიტეტო ქსელის, სერვისებისა და მოწყობილობების საიმედოობას, უსაფრთხოებას, მთლიანობას და ხელმისაწვდომობას.

მუხლი 12. დაზიანების აღმოფხვრა

12.1. ნებისმიერი ხარვეზის (ნებისმიერი მოვლენა, რომელიც ხელს უშლის ბიზნესუწყვეტობს ან/და უზღუდავს მომხმარებლებს მათთვის განსაზღვრულ ლოკალურ ან გლობალურ რესურსთან წვდომას) გამოსწორება ხდება დაუყოვნებლივ.

12.2. პროცესების მიმდინარეობის ეტაპობრივი სტრუქტურა შემდეგია:

ა) შეტყობინება დაზიანების შესახებ (სატელეფონო და/ან ელ. ფოსტის საშუალებით);

ბ) ოპერატორი მართვის პანელიდან ახდენს დაზიანების იდენტიფიცირებას და აღმოფხვრას;

გ) ოპერატორი საჭიროების შემთხვევაში მიდის დაზიანების ადგილზე;

დ) თუ ოპერატორის მიერ ვერ ხერხდება დაზიანების აღმოფხვრა, ატყობინებს ადმინისტრატორს;

ე) ადმინისტრატორი ატარებს ქსელის დიაგნოსტიკას;

ვ) ჩასატარებელი სამუშაოების შესახებ აცნობებს ოპერატორს.

ზ) ოპერატორი ატყობინებს მომხმარებელს დაზიანების და გამოსწორების სავარაუდო ვადების შესახებ.

მუხლი 13. ინფორმაციული ტექნოლოგიებისა და ინფორმაციული უსაფრთხოების აუდიტი

13.1. ინფორმაციული ტექნოლოგიების გამართულად ფუნქციონირების, ინფორმაციული უსაფრთხოების უზრუნველყოფისა და ინფორმაციული სისტემების მუშაობის გაუმჯობესებისთვის რელევანტური ინფორმაციის მოძიების მიზნით, უნივერსიტეტი პერიოდულად ატარებს ინფორმაციული ტექნოლოგიებისა და ინფორმაციული უსაფრთხოების აუდიტს.

13.2. აუდიტი ტარდება სულ ცოტა წელიწადში ერთხელ. აუდიტის ვადებსა და ჩართულ პირთა წრეს განსაზღვრავს რექტორის მოადგილე ადმინისტრაციული და საფინანსო მიმართულებით.

13.3. აუდიტის ჩატარების მიზნით იქმნება აუდიტის კომისია, რომელშიც შესაძლებელია შედიოდნენ უნივერსიტეტის პერსონალი და გარე მოწვეული სპეციალისტები.

13.4. აუდიტის შედეგად კომისია შეიმუშავებს დასკვნას ინფორმაციული უსაფრთხოების გამოვლენილი დარღვევებისა და პროცესების გასაუმჯობესებლად ორიენტირებული რეკომენდაციების ჩამონათვალს.

13.5. აუდიტის კომისიის რეკომენდაციების შესრულებაზე პასუხისმგებლობა ეკისრება რექტორის მოადგილეს ადმინისტრაციული და საფინანსო მიმართულებით.

მუხლი 14. პოლიტიკის იმპლემენტაცია და კონტროლი მის შესრულებაზე

14.1. წინამდებარე პოლიტიკით განსაზღვრული წესების, პროცედურებისა და ვალდებულებების შესრულებაზე კონტროლს ინფორმაციული ტექნოლოგიების სამსახურის მიერ მოწოდებული ინფორმაციის საფუძველზე ახორციელებს უნივერსიტეტის რექტორის მოადგილე ადმინისტრაციული და საფინანსო მიმართულებით.

14.2. ცალკეული საკითხის შესწავლის მიზნით, მისი სირთულიდან გამომდინარე, რექტორის მოადგილე უფლებამოსილია მიმართოს რექტორს დროებითი სამუშაო ჯგუფის შექმნისა და შესაბამისი საკითხის შესწავლის ვალდებულების მასზე დაკისრების თაობაზე.

14.3. კონტროლის ღონისძიებებთან ერთად, ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის კოორდინირებით ხორციელდება ინფორმაციული ტექნოლოგიების ეფექტური ფუნქციონირებისა და ინფორმაციული უსაფრთხოების ნაწილში პერსონალის ცნობიერების ამაღლების ღონისძიებები, ტრენინგები, საინფორმაციო შეხვედრები და საინფორმაციო მასალების მომზადება.

მუხლი 15. პასუხისმგებლობა ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის მოთხოვნების დარღვევაზე

15.1. წინამდებარე პოლიტიკის მოთხოვნათა შეუსრულებლობა მიიჩნევა დასაქმებულის მიერ სამუშაო პირობების დარღვევად და განიხილება უნივერსიტეტის შინაგანაწესით დადგენილი პროცედურით.

15.2. წინამდებარე პოლიტიკით გათვალისწინებული ინფორმაციული ტექნოლოგიების მართვის ან ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევა, რომლის შედეგად არ დამდგარა ქონებრივი ან არაქონებრივი ზიანი, მიიჩნევა დასაქმებულის მიერ სამუშაო პირობების მსუბუქ დარღვევად.

15.3. მსუბუქი დარღვევის შემთხვევაში დასაქმებულს შესაძლებელია მიეცეს ზეპირი ან წერილობითი შენიშვნა/გაფრთხილება, ამასთან, შესაძლებელია გატარდეს დასაქმებულის ინფორმაციული წიგნიერების განვითარების ღონისძიებები.

15.4. წინამდებარე პოლიტიკით გათვალისწინებული ინფორმაციული ტექნოლოგიების მართვის ან ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევა, რომლის შედეგად დადგა ქონებრივი ან არაქონებრივი ზიანი, მიიჩნევა დასაქმებულის მიერ სამუშაო პირობების მნიშვნელოვან დარღვევად, და შესაძლებელია გახდეს მის მიმართ დისციპლინარული პასუხისმგებლობის საკითხის დაყენების საფუძველი, უნივერსიტეტის შინაგანაწესით დადგენილი წესით.

15.5. მიყენებული ზიანის კომპენსაციის საკითხი წყდება საქართველოს სამოქალაქო კოდექსის, შრომის კოდექსისა და უნივერსიტეტის შინაგანაწესით გათვალისწინებული წესით.

15.6. დარღვევის განმეორების, ან განსაკუთრებით უხეში ან დიდი ზიანის მქონე დარღვევის შემთხვევაში, შესაძლებელია დადგეს დასაქმებულთან შრომითი ხელშეკრულების შეწყვეტის საკითხი, უნივერსიტეტის სამართლებრივი აქტებით და დასაქმებულთან გაფორმებული შრომითი ხელშეკრულებით გათვალისწინებული პროცედურით.

15.7. წინამდებარე პოლიტიკით გათვალისწინებული ინფორმაციული ტექნოლოგიების მართვის ან ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევა, რომელიც სავარაუდოდ შეიცავს ადმინისტრაციული გადაცდომის ან სისხლის სამართლებრივი დანაშაულის ნიშნებს, გამოძიებული უნდა იყოს კანონმდებლობით დადგენილი წესით.

მუხლი 16. დასკვნითი დებულებები

16.1. უნივერსიტეტის წესდების შესაბამისად, პოლიტიკის პირველი რედაქცია მიღებულია და დამტკიცებულია უნივერსიტეტის პარტნიორთა კრების მიერ.

16.2. პოლიტიკა ძალაში შედის პარტნიორთა კრების მიერ მისი დამტკიცებისთანავე.

16.3. პოლიტიკის მოდიფიცირებული რედაქციის, მასში ცვლილებებისა და დამატებების დამტკიცებას ადმინისტრაციული და საფინანსო მიმართულებით რექტორის მოადგილის წარდგინების საფუძველზე უზრუნველყოფს უნივერსიტეტის რექტორი.

16.4. პოლიტიკაში ცვლილებები და დამატებები ძალაში შედის უნივერსიტეტის რექტორის მიერ მისი დამტკიცებისთანავე, თუ რექტორის ბრძანებით არ იქნება განსაზღვრული ცვლილების ძალაში შესვლის განსხვავებული სამომავლო თარიღი.