თბილისის ღია სასწავლო უნივერსიტეტი

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და ინფრასტრუქტურა

(დამტკიცებულია აკადემიური და წარმომადგენლობითი სენატის 2018 წლის 22 იანვრის #77 დადგენილებით)

შინაარსი

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს თბილისის ღია სასწავლო უნივერსიტეტში (შემდგომში - უნივერსიტეტი) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს უნივერსიტეტის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში, სასწავლო პროცესის მართვის ელექტრონული სისტემა emis.openuni.edu.ge -ს ადმინისტრირებისა და გამოყენების წესებს.
2. წინამდებარე წესის შესაბამისი ნაწილების დაცვა სავალდებულოა ყველა იმ პირისთვის, რომლებიც თავის ადმინისტრაციულ, აკადემიურ თუ სტუდენტის საქმიანობაში იყენებს უნივერსიტეტის ინფორმაციულ ტექნოლოგიებსა და რესურსებს .
3. უნივერსიტეტის საინფორმაციო ტექნოლოგიების მომხმარებელი (შემდეგში - მომხმარებელი) ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

თავი I - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა შემუშავებულია რათა უზრუნველყოს თბილისის ღია სასწავლო უნივერსიტეტში სატელეკომუნიკაციო ქსელის საიმედოობა, უსაფრთხოება, მთლიანობა და ხელმისაწვდომობა. ხელი შეუწყოს უნივერსიტეტის საგანმანათლებლო, ადმინისტრაციული და ბიზნეს პროცესების შეუფერხებელ მიმდინარეობას.
2. პოლიტიკას ახორციელებს საინფორმაციო ტექნოლოგიების სამსახური (შემდგომში ,,სამსახური“), რომელიც ვალდებულია:
ა) მომხმარებლები უზრუნველყოს ჯგუფისთვის წინასწარ განსაზღვრული რესურსებით, გააცნოს მათი ექსპლუატაციის წესები.
ბ) დარღვევის შემთხვევაში დროებით შეუჩეროს ან შეუწყვიტოს რესურსთან წვდომა.
გ) ტექნოლოგიების, სტანდარტებისა და სერვისების სამომავლო განვითარებასა და ცვლილებასთან ერთად, შეიმუშავოს, დანერგოს და მართოს ახალი ინფორმაციული ტექნოლოგიების რესურსები.
3. ახალი სერვისის, მოწყობილობის, ქსელის და ტექნოლოგიის დანერგვა ან/და არსებულის ცვლილება უნდა შეესაბამებოდეს თბილისის ღია სასწავლო უნივერსიტეტის განვითარების პოლიტიკას და არ უნდა ეწინააღმდეგებოდეს ელექტრონული სისტემების მართვის პოლიტიკას.
4. გარდა ადმინისტრატორისა და ოპერატორისა არავის აქვს უფლება თვითნებურად დაუკავშიროს თბილისის ღია უნივერსიტეტის ქსელს მოწყობილობა, ხელოვნურად გააფართოვოს მისი დაფარვის არეალი ან განახორციელოს ნებისმიერი სხვა საქმიანობა, რომელიც არღვევს საუნივერსიტეტო ქსელის, სერვისებისა და მოწყობილობების საიმედოობას, უსაფრთხოებას, მთლიანობას და ხელმისაწვდომობას.

მუხლი 3. . უსაფრთხოების პოლიტიკა

1. საინფორმაციო ტექნოლოგიების რისკების მართვის მიზნით სამსახური ატარებს უსაფრთხოების პოლიტიკას, რომლის დაცვის სფეროებს წარმოადგენს:

ა) უნივერსიტეტის IT ინფრასტრუქტურა;

ბ) უნივერსიტეტში არსებული ძირითადი მონაცემები და ინფორმაცია;

გ)პირები, რომლებიც იყენებენ ინფორმაციულ სისტემებს ან ახორციელებენ მის ადმინისტრირებას;

დ) პირები, რომლებიც ახორციელებენ ძირითადი მონაცემებისა და ინფორმაციის მართვას.

2. უსაფრთხოების პოლიტიკა განსაზღვრავს:

ა)უნივერსიტეტის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;

ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

3. უნივერსიტეტის ინფორმაციული ტექნოლოგიების (IT) სამსახური ვალდებულია 24 საათიან რეჟიმში 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.

4. ფიზიკური უსაფრთხოება

1. უნივერსიტეტი ახორციელებს კონტროლს ინფორმაციულ აქტივებზე არაავტორიზებული წვდომის, ჩარევის, დატაცებისა ან დაზიანების თავიდან ასაცილებლად.

2. სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ფიზიკური, ტექნიკური, პროცედურული და გარემოს უსაფრთხოების კონტროლის მექანიზმებით.

3. უნივერსიტეტი ახორციელებს ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის და/ან მგრძნობელობის ინფორმაციას. ასეთი მოწყობილობები განთავსებულია ფიზიკურად დაცულ ადგილას.

5. **ინფორმაციული უსაფრთხოების ინციდენტები**

1.უნივერსიტეტი ვალდებულია განახორციელოს უსაფრთხოების ინციდენტების იდენტიფიცირება, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას.

2.უნივერსიტეტის ინფორმაციული ტექნოლოგიების სისტემის ფუნქციონირებაზე პასუხისმგებელი პირები პერიოდულად წარმოადგენენ ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების, მათი წყაროების (შიდა, გარე) მათი ფორმების (DDoS, Keylog და სხვა) მიხედვით, გამოსწორებისა და ოპტიმიზაციის რეკომენდაციებთან ერთად.

მუხლი. 4 მომხმარებლების მართვის პოლიტიკა

1. მომხმარებლები იყოფიან ჯგუფებად და სარგებლობენ მათთვის გამოყოფილი ფიზიკური თუ ელექტრონული მოწყობილობებითა და სერვისებით. სპეციფიკიდან გამომდინარე არსებობს ჯგუფის შიდა დამატებითი წვდომის დონეები.

2.მომხმარებლების ჯგუფებისა და დონეების განსაზღვრა/ცვლილება ხდება წინასწარ, ინფორმაციული ტექნოლოგიების სამსახურის და უნივერსიტეტის ადმინისტრაციის უფროსთან ან მოვალეობის შემსრულებლებთან შეთანხმებით.

3.მომხმარებლების ჯგუფებისა და დონეების შეუსაბამო ქმედება გამოიწვევს:

ა) მოწყობილობებთან და ელექტრონულ სერვისებთან წვდომის შეზღუდვას;

ბ) საუნივერსიტეტო ქსელიდან განცალკევებას ან/და იზოლირებას.

4. დაშვების წერტილების ფუნქციური ჯგუფები და მართვის პოლიტიკა

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

❖ **ქსელის, მოწყობილობებისა და სერვისების მართვის ჯგუფი:**

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

❖ **თანამშრომლების ჯგუფი:**

ჯგუფი განკუთვნილია უნივერსიტეტის თანამშრომლებისთვის და დაშვეულია მოწყობილობებს შორის ინფორმაციის ურთიერთგაცვლა. შეზღუდულია სხვა ჯგუფებთან კომუნიკაცია.

❖ **სტუმრებისა და სტუდენტების ჯგუფი:**

ჯგუფი განკუთვნილია სტუმრებისთვის და სტუდენტებისთვის და დაშვება აქვს მხოლოდ განსაზღვრულ ინტერნეტ სერვისებთან შეზღუდული დროით.

❖ **უსაფრთხოებისა და ტელეფონიის ჯგუფი:**

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

❖ **საგამოცდო და ლაბორატორიული ჯგუფი:**

ჯგუფი განკუთვნილის ელექტონული გამოცდებისა და ლაბორატორიული საქმიანობისთვის. დაშვებულია მხოლოდ საგამოცდო და ლაბორატორიულ რესურსთან წვდომა. შეზღუდულია სხვა ჯგუფებთან და ცალკეულ სერვისებთან წვდომა.

მუხლი 5. კომუნიკაციებისა და ოპერაციების მართვა

1. უნივერსიტეტი ახორციელებს მუდმივ კონტროლს ინფორმაციის დამამუშავებელ და გადამცემ მოწყობილობებზე მათი სწორი და უსაფრთხო სარგებლობის უზრუნველყოფის მიზნით.

2. სატელეკომუნიკაციო კვანძებთან წვდომა:

სატელეკომუნიკაციო კვანძებთან წვდომა იზღუდება ყველასთვის ოპერატორის და ადმინისტრატორის გარდა. უსაფრთხოების მიზნით დაკეტილია, როგორც სატელეკომუნიკაციო შახტა, ასევე კარადა (გამონაკლისია კომპიუტერული ოთახები, სადაც სატელეკომუნიკაციო

კარადა განთავსებულია უშუალოდ ოთახში და არა შახტაში). აპარატურასთან წვდომისთვის საჭიროა:

ა) დაშვების მიზნის და საჭიროების შეტყობინება ადმინისტრაციისთვის წერილობით;

ბ) უსაფრთხოების სამსახურის შეტყობინება სატელეკომუნიკაციო შახტასთან წვდომისთვის;

გ) ოპერატორის შეტყობინება სატელეკომუნიკაციო კარადასთან წვდომისთვის;

დ) სამუშაოს დასრულების შემდეგ ოპერატორის და უსაფრთხოების სამსახურის შეტყობინება.

3. დაზიანების აღმოფხვრა

ქსელის მონიტორინგი ხორციელდება 24 საათიან რეჟიმში, სწორედ ამიტომ ნებისმიერი ხარვეზის (ხარვეზში იგულისხმება ნებისმიერი მოვლენა რომელიც ხელს უშლის ბიზნეს უწყვეტობს ან/და უზღუდავს მომხმარებლებს მათთვის განსაზღვრულ ლოკალურ ან გლობალურ რესურსთან წვდომას) გამოსწორება ხდება დაუყოვნებლივ.

პროცესების მიმდინარეობის ეტაპობრივი სტრუქტურა შემდეგია:

- შეტყობინება დაზიანების შესახებ;
- ოპერატორი მართვის პანელიდან ახდენს დაზიანების იდენტიფიცირებას და აღმოფხვრას;
- ოპერატორი საჭიროების შემთხვევაში მიდი დაზიანების ადგილზე;
- თუ დაზიანების აღმოფხვრა მაინც ვერ მოხერხდა, ატობინებს ადმინისტრატორს;
- ადმინისტრატორი ატარებს ქსელის დიაგნოსტიკას;
- ჩასატარებელი სამუშაოების შესახებ აცნობებს ოპერატორს;
- ოპერატორი ატყობინებს მომხმარებელს დაზიანების და გამოსწორების სავარაუდო ვადების შესახებ.

მუხლი 6. ახალი სისტემის დაგეგმვა შემუშავება

სისტემების დაგეგმვისა და დანერგვის პროცესში გათვალისწინებულ უნდა იქნეს სისტემების ტექნიკური და ფუნქციური შესაძლებლობები, რათა არ მოხდეს კრიტიკული სისტემების გამართული მუშაობის შეფერხება.

მუხლი 7. საზიანო პროგრამებზე კონტროლი

საზიანო ან თაღლითური პროგრამების გამოყენების თავიდან აცილების მიზნით აუცილებელია კრიტიკულ სისტემებზე კონტროლის განხორციელება.

მუხლი 8. ვირუსებისგან დაცვა

1.უნივერსიტეტი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება უნივერსიტეტის შიგნით და უნივერსიტეტის მიზეზით – მის გარეთ;

მუხლი 9. სისტემები, აპლიკაციები და მონაცემთა სარეზერვო ასლები

ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება სინქრონულად უნივერსიტეტის google drive - ზე.

მუხლი 10. კომპიუტერული ქსელის მართვა

1. უნივერსიტეტში, როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილებების mac მისამართები, რომლებიც განეკუთნებიან უნივერსიტეტის აქტივებს წინასწარ არის გაწერილი როუტერში, რომელიც ანიჭებს წინასწარ შერჩეულ Ip მისამართს.

2. ისეთი მოწყობილობები, რომლებიც არ განეკუთნებიან უნივერსიტეტის აქტივებს და იყენებენ უნივერსიტეტის უკაბელო ქსელს (wifi), სარგებლობენ სპეციალური გამოყოფილი ქსელით,

რომლის საშუალებითაც შეუძლიათ წვდომა ჰქონდეთ მხოლოდ დაშვებულ ვებ გვერდების კატეგორიასთან, რომლებიც წინასწარ შერჩეულია.

თავი II - უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონული სისტემა

მუხლი 11. სასწავლო პროცესის მართვის ელექტრონული სისტემის აღწერა

1. უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონული სისტემა emis.openuni.edu.ge უზრუნველყოფს უნივერსიტეტის საგანმანათლებლო და ადმინისტრაციულ საქმიანობაში არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.

2. სისტემის ზოგადი ფუნქციები:

ა) უნივერსიტეტში სასწავლო პროცესის მართვის ავტომატიზაცია;

ბ) ფინანსური მოდულის ავტომატიზაცია;

გ) ელექტრონულ საქმის წარმოება.

3.სისტემაში გამოყენებულია კრიპტოგრაფია, სადაც დაშიფრულია მომხმარებლების (ადმინისტრაცია, პროფესორ/მასწავლებელი, სტუდენტი) პაროლები.

4. სისტემის მომხმარებლებია:

ა) ადმინისტრაცია;

ბ) პროფესორ/მასწავლებელი;

გ) სტუდენტი.

მუხლი 12 . ელექტრონული სერვისები

1. სასწავლო პროცესის მართვის ელექტრონული სისტემა აერთიანებს შემდეგ სერვისებს (მოდულებს):

- ❖ სასწავლო პროცესი;
- ❖ საფინანსო სერვისი;
- ❖ ბიბლიოთეკის სერვისი;
- ❖ ელექტრონული საქმის წარმოება;
- ❖ საკომუნიკაციო სერვისი.

2. სასწავლო პროცესი

სერვისი მოიცავს: სტუდენტების რეესტრს, სტუდენტის აკადემიური მოსწრების ინფორმაციის შეტანა/დამუშავებას, სასწავლო კურსების რეესტრს (კრედიტი, წინაპირობა), საგანმანათლებლო პროგრამების კატალოგს, სილაბუსების ატვირთვას, ლექტორის და სტუდენტის ინდივიდუალურ პანელს.

შედეგად:

ა) არსებული მონაცემების გადამუშავების ფორმირდება სხვდასხვა საბეჭდი ფორმები (ნიშნების ფურცელი, ცნობა, ფორმა 26, უწყისი), სტატისტიკური რეპორტები.

ბ) სტუდენტს საკუთარ გვერდზე აქვს აქვს წვდომა: საგანმანათლებლო პროგრამაზე, სასწავლო კურსების სილაბუსებზე, საკუთარ აკადემიურ შეფასებაზე, რაც უზრუნველყოფს ინფორმაციის ხელმისაწვდომობას.

გ) სტუდენტი განახორციელებს აკადემიურ რეგისტრაციას და თავად დაგეგმავს საკუთარ აკადემიურ კალენდარ, დარეგისტრირდება სასურველ დროს და სასურველ სასწავლო კურსებზე (რასაც ითვალისწინებს სტუდენტის სასწავლო პროგრამა, სასწავლო კურსების წინაპირობების დაცვით), რაც უზრუნველყოფს სტუდენტუს აკადემიურ თავისუფლებას.

დ) პროფესორ/მასწავლებლების რეესტრი ასახავს პროფესორ/მასწავლებლების პირად მონაცემებს და თანამდებობებს.

ე) პროფესორ/ მასწავლებლეის სისტემის მეშვეობით გაუწევენ კონსულტაციებს სტუდენტებს ელექტრონულად და აუტვირთავენ სხდავსხვა ელექტრონულ დოკუმენტაციას.

3. საფინანსო სერვისი

სერვისი მოიცავს: სტუდენტების გადასხადის გრაფიკებს, გრანტებს, ტრანზაქციებს.

შედეგად:

ა) სტუდენტს აქვს ინფორმაცია მის ფინანსურ ვალდებულებებზე, გადახდის გრაფიკზე;

ბ) უფლებამოსილ სუბიექტს შეუძლია ეფექტურად მართოს სერვისის დახმარებით საფინანსო პროცესი უნივერსიტეტში.

4. **ბიბლიოთეკის სერვისი**

სერვისის საშუალებით უნივერსიტეტში ხორციელდება ელექტრონული და მატერიალური ფონდის კატალოგიზაცია, შესაძლებელია წიგნების გაცემა ბიბლიოთეკის მომხმარებელზე, დავალიანებული (ვადაგადაცილებული) წიგნების აღირცხვა, ელექტრონული წიგნების ატვირთვა, ამასთანავე, სტუდენტს და პროფესორ/მასწავლებლებს აქვთ შესაძლებლობა საკუთარი გვერდებიდან მიიღონ ინფრმაცია უნივერსიტეტის ბიბლიოთეკაში არსებულ როგორც წიგნად ფონდზე, ასევე ელექტრონულ რესურსზე.

5. ელექტრონული საქმის წარმოება

სერვისის საშალებით უნივერსიტეტში ხორციელდება დოკუმენტ ბრუნვა, შემოსული და გასული კორესპოდენციის აღიცხვა, ელექტრონული დოკუმენტების ატვირთვა, ამასთანავე, სტუდენტებს აქვთ შესაძლებლობა, ელექტრონულად დაწერონ სასურველი განცხადება უნივერსიტეტში მიუსვლელად.

6. საკომუნიკაციო სერვისი

სერვისი აძლევს საშუალებას ადმინისტრაციას, პროფესორ/მასწავლებლებს და სტუდენტებს ჰქონდეთ ელექტრონული კომუნიკაცია, მ.შ. სასურველი ელექტრონული მასალების გადაცემის შესაძლებლობა.

მუხლი 13. სასწავლო პროცესის მართვის ელექტრონული სისტემის ეფექტურობა

1. უნივერსიტეტში მოქმედი ელექტრონული სერვისები იძლევა საშუალებას ეფექტურად განხორციელდეს და უზრუნველყოფილი იყოს:

ა) სტუდენტის ინფორმაციის მოძიება;

ბ) სტუდენტზე ინფორმაციის შექმნა;

გ) სხვდასხვა რეპორტების (სტუდენტის სტატუსები, ფინანსური დავალიანებები, GPA რეიტინგი დასხვა) ამოღება;

დ) უნივერსიტეტში არსებულ ინფორმაციაზე სტუდენტის წვდომა ნებისმიერი ადგილიდან;

ე) სტუდენტის აკადემიური თავისუფლების რეალიზაცაი;

ვ) კომუნიკაცია - პროფესორ/მასწავლებლები, ადმინისტრაცია, სტუდნეტი;
ზ) ელექტრონული მასალების გაცვლა;
თ) სხვდასხვა საბეჭდი ფორმების ბეჭდვა;
ი) სასწავლო კურსებზე წინაპირობების ავტომატური დაცვა;
კ) საგანმანათლებლო პროგრამების ხელმისაწვდომობა;
ლ) სილაბუსის ხელმისაწვდომობა;
მ) შეფასების სისტემაში მინიმალური და მაქსიმალური ზღვრების ავტომატური დაცვა.

მუხლი 14. სასწავლო პროცესის მართვის ელექტრონული სისტემის განვითარება

1. სისტემის განვითარებაზე პასუხისმგებელია საინფორმაციო ტექნოლოგიების სამსახური. **5.** სისტემის განვითარების (სისტემაში ახალი ფუქნციის დამატება /განახლების) საფუძველი შეიძლება იყოს:
ა) საკონონმდებლო ცვლილება;
ბ) ადმინისტრაციისა და პროფესორ/მასწავლებლების ინიციატივები;
გ) სტუდენტების ინიციატივები.

2. სისტემის განვითარება იწვევს როგრამული კოდის ცვლილებას, რომელიც განხორციელდება საინფორმაციო ტექნოლოგიების სამსახურის მიერ რექტორთან/ვიცე-რექტორთან შეთანხმებით.

მუხლი 15. სისტემაში ინფორმაციის ცვლილება

7. სისტემაში არსებული ინფორმაციის ცვლილება ხდება რექტორის/ ვიცე-რექტორის გადაწყვეტილების საფუძველზე საინფორმაციო ტექნოლოგიების სამსახურის მიერ.

მუხლი 16. სისტემის უსაფრთხოება

1. სისტემის კოდი იწერება სპეციალურად გამოყოფილ ლოკალურ სერვერზე, სადაც ხდება სისტემაში დამატებული ახალი მოდულის ტესტირება შემდეგ ხდება შემოწმებული კოდის ატვირთვა ძირითად სერვერზე
2. სერვერზე ინახება მოქმედებათა ლოგები, შემდეგი მონაცემებით: მოქმედების ავტორი, მოქმედების დრო, შესრულებული მოქმედება, IP მისამართი
3. ბიზნესის უწყვეტობის მიზნით, ძირითადი სერვერის მწყობრიდან გამოსვლის შემთხვევაში, ავტომატურად ირთვება სარეზერვო სერვერი, რომელიც ახდენს რეაპლიკაციას ძირითად სერვერთან.
4. სისტემის მონაცემები დღეში ერთხელ ავტომატურად ინახება უნივერსიტეტის google drive ზე.
5. სასწავლო პროცესის მართვის სისტემის უსაფრთხოებაზე პასუხისმგებელია INI.GE ჯგუფი. INI.GE ჯგუფი ვალდებულია ყოველი კვირის ბოლოს, გაუგზავნოს დარეზერვებული ფაილები (Beckup) თბილისის ღია სასწავლო უნივერსიტეტის IT სამსახურს. IT სამსახური ვალდებული მიღებული დარეზერვებული ფაილები (Beckup) განათავსოს ღრუბელში (Cloud).

თავი IV- საინფორმაციო ქსელის ინფრასტრუქტურა

მუხლი 17. საინფორმაციო ქსელის ინფრასტრუქტურა

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

2. სატელეკომუნიკაციო ინფრასტრუქტურის დაგეგმარება და მონტაჟი მოხდა სუნივერსიტეტო შენობის მშენებლობასთან ერთად და მაქსიმალურად გათვლილია უახლოესი 8-10 წლის განმავლობაში ტექნოლოგიების განვითარებასთან ადაპტირებისთვის.

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

4. დაშვების წერტილები და ტექნოლოგიები

უნივერსიტეტის შენობის ტერიტორიაზე ყველა ოთახში განთავსებულია ფიზიკური დაშვების წერტილები და აგრეთვე შესაძლებელია რადიოსიხშირული სპექტრით სარგებლობა.

ქსელთან დაშვების უსადენო ტექნოლოგია:

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

ქსელთან დაშვების სადენიანი ტექნოლოგია:

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.

ქსელთან დაშვების VPN ტექნოლოგია:

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

ქსელთან დაშვების უსაფრთხოება:

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

5. სამეთვალყურეო სისტემა

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

სამეთვალყურეო სისტემის უსაფრთხოება:

სამეთვალყურეო ქსელი წარმოადგენს დახურულ სისტემას, რომელთან წვდომა ცვლილება/ჩაწერის რეჟიმში იზღუდება ყველასთვის, ხოლო წაკითხვის რეჟიმში ხელმისაწვდომია მხოლოდ უსაფრთხოების სამსახურისთვის.

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

ტელეფონი:

უნივერსიტეტის ტერიტორიაზე დანერგილია VoIP ტექნოლოგიაზე დაფუძნებული ტელეფონიის სისტემა, რომელიც უზრუნველყოფს თანამშრომელთა ერთმანეთთან და აგრეთვე საქართველოს

ტერიტორიაზე არსებულ სხვადასხვა სახაზო სატელეფონო ოპერატორების აბონენტებთან შეუფერხებელ კომუნიკაციას.

სატელეფონო სისტემის უსაფრთხოება:

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.

6. **სარეზერვო სისტემები**

ბიზნეს უწყვეტობის უზრუნველსაყოფად უნივერსიტეტში დანერგილია სხვადასხვა სარეზერვო სისტემები:

❖ ფიზიკური სარეზერვო სისტემა: უნივერსიტეტს აქვს სთორეიჯ სერვერი რომელიც მუშაობს რაიდ 10-ში. რაც მნიშვნელოვანია სერვერზე განთავსებული დოკუმენტების უსაფრთხოებისთვის.

❖ ელექტრონული სარეზერვო სისტემა: სერვერზე ყოველი დღის ბოლოს ავტომატურად კეთდება ფაილების რეზერვი (Beckup) Google Drive-ზე.

❖ **ინტერნეტ სერვისის სარეზერვო სისტემა:**

თბილისის ღია სასწავლო უნივერსიტეტს ემსახურება ორი ინტერნეტ პროვაიდერი. მაგთიკომი და გრენა. ძირითად ინტერნეტის წყაროდ გამოყენებულია გრენას ხაზი. მაგთიკომის ხაზი რეზერვშია.

❖ **კვების სარეზერვო სისტემა:**

ელექტრო ენერგიის უწყვეტი მიწოდებისთვის უნივერსიტეტს გააჩნია 74 კილოვატიანი დიზელის გენერატორი , რომელიც დენის წასვლიდან 4 წამში ირთვება ავტომატურად. ასევე უნივერსიტეტის სტაფი აღჭურვილია დენის სარეზერვო სისტემით (UPS).