საქართველოს ეროვნული უნივერსიტეტი სეუ
GEORGIAN NATIONAL UNIVERSITY SEU

საქართველოს ეროვნული უნივერსიტეტი სეუ-ს ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

დამტკიცებულია
რექტორის 2020 წლის 20 ივლისის №412 ბრძანებით

თბილისი
2020

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს საქართველოს ეროვნული უნივერსიტეტი სეუ-ში (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 reg.seu.edu.ge-ს და emis.seu.edu.ge - ს ადმინისტრირებისა და გამოყენების წესებს.
2. წინამდებარე წესის 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 უსაფრთხოების პოლიტიკა უზრუნველყოფს უნივერსიტეტში ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.
2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:
   ა) უნივერსიტეტის ი.ტ/ი.ს 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.
3. პოლიტიკა განსაზღვრავს:
   ა) უნივერსიტეტის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;
   ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 3. 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.

მუხლი 4. 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 5. კომუნიკაციებისა და ოპერაციების მართვა

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

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

მუხლი 9. კომპიუტერული ქსელის მართვა

1. უნივერსიტეტში როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილებების mac მისამართები, რომლებიც განეკუთნებიან უნივერსიტეტის აქტივებს წიანსწარ 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 ვებგვერდების კატეგორიასთან, რომლებიც წინასწარ შერჩეულია.

მუხლი 10. სისტემების უსაფრთხოება ტესტირებისა და შექმნის პროცესში

სისტემების ტესტირება ხდება იზოლირებულ გარემოში, რათა სასიცოცხლოდ მნიშვნელოვანი კრიტიკული სისტემები დაცულ იქნეს შეცდომით განადგურების და/ან დაზიანებისაგან.

მუხლი 11. ბიზნესუწყვეტობის მართვა

1. ბიზნესისუწყვეტობის შემუშავებულმა სტრატეგიამ და მისმა ფუნქციონირებამ უნდა უზრუნველყოს უნივერსიტეტის ინფორმაციის დამუშავების პროცესში მოულოდნელი წყვეტის რისკის შემცირება და მოახდინოს მისი დროული აღდგენა.
2. ძირითადი როუტერის მწყობრიდან გამოსვლის შემთხვევაში ხდება სარეზერვო როუტერის ჩართვა, შედეგის დადგომიდან 10 წუთის განმავლობაში.
3. გარე სერვერების მწყობრიდან გამოსვლის შემთხვევაში, 5 წუთში ხდება მათი სარეზერვო ასლების გააქტიურება, რათა არ შეფერხდეს ელექტრონული სერვისები.

თავი II - უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონული სისტემა

მუხლი 12. სასწავლო პროცესის მართვის სისტემის აღწერა

1. უნივერსიტეტის ელექტრონული სერვისების სისტემა reg.seu.edu.ge უზრუნველყოფს უნივერსიტეტის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციას დამუშავებასა და დაცვას.
2. სისტემის ზოგადი ფუნქციები:
   ა) უნივერსიტეტში სასწავლო პროცესის მართვის ავტომატიზაცია;

ბ) ფინანსური მოდულის ავტომატიზაცია;

გ) ელექტრონული საქმის წარმოება;

დ) ბიბლიოთეკა;

ე) ადამიანური რესურსების მართვა

3. სისტემაში გამოყენებულია md5s ტიპის კოდირება, სადაც დაშიფრულია მომხმარებლების (პერსონალი, სტუდენტი) პაროლები.

4. სისტემის მომხმარებლებია:

ა) ადმინისტრაციული, აკადემიური და მოწვეული პერსონალი;

ბ) სტუდენტი.

მუხლი 12. სისტემის უსაფრთხოება

1. სისტემის კოდი იწერება სპეციალურად გამოყოფილ ლოკალურ სერვერზე, (https://bitbucket.org/) 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 რეპლიკაციას ძირითად სერვერთან.

4. სისტემის მონაცემები დღეში ერთხელ ავტომატურად ინახება უნივერსიტეტის google drive ზე.

5. გარე სერვერების რეზერვაცია, რომლებიც ემსახურებიან ელექტრონული სერვისების მართვის სისტემას, ხდება 2-ჯერ დღის განმავლობაში.

მუხლი 13. განვითარების მექანიზმები

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

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

3. უნივერსიტეტი უზრუნველყოფს საინფორმაციო რესურსების განვითარებას, გაუმჯობესებას და პროცესების ოპტიმიზაციისა და მონიტორინგს, როგორც ადმინისტრაციაში პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუთსორსინგით.