შპს თბილისის დავით აღმაშენებლის სასწავლო უნივერსიტეტი

დამტკიცებულია:

შპს თბილისის დავით აღმაშენებლის სასწავლო უნივერსიტეტის აკადემიური საბჭოს გადაწყვეტილებით რექტორი: ანზორ შარაშენიძე

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

2019 წ.

თავი 1 - ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს შპს თბილისის სასწავლო უნივერსიტეტის (შემდგომში - სასწავლო უნივერსიტეტი) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს სასწავლო უნივერსიტეტის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში, სასწავლო პროცესის მართვის ელექტრონული სისტემის 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. სასწავლო უნივერსიტეტის საინფორმაციო ტექნოლგოებიების მომხმარებელი (შემდეგში - მომხმარებელი) ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები ინტეელქტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს სასწავლო უნივერსიტეტში ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.
2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:

ა) სასწავლო უნივერსიტეტის ი.ტ/ი.ს ინფრასტრუქტურა

ბ) სასწავლო 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) სასწავლო უნივერსიტეტის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;

ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 3. ფიზიკური უსაფრთხოება

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

2. სასწავლო 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

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

მუხლი 6. ახალი სისტემის დაგეგმვა შემუშავება

1. 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

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

მუხლი 8. ვირუსებისგან დაცვა

1. სასწავლო უნივერსიტეტი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება უნივერსიტეტის შიგნით და უნივერსიტეტის მიზეზით – მის გარეთ; სისტემები, აპლიკაციები და მონაცემთა სარეზერვო ასლები
2. ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება სინქრონულად უნივერსიტეტის google drive - ზე.

მუხლი 9. კომპიუტერული ქსელის მართვა

1. სასწავლო უნივერსიტეტში როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილებების mac მისამართები რომლებიც

განეკუთნებიან სასწავლო უნივერსიტეტის აქტივებს წიანსწარ არის გაწერილი როუტერში, რომელიც ანიჭებს წინასწარ შერჩეულ Ip მისამართს.

2. ისეთი მოწყობილობები, რომლებიც არ განეკუთნებიან უნივერსიტეტის აქტივებს და იყენებენ სასწავლო უნივერსიტეტის უკაბელო ქსელს (wifi), სარგებლობენ სპეციალური გამოყოფილი ქსელით, რომლის საშუალებითაც შეუძლიათ წვდომა ჰქონდეთ მხოლოდ დაშვებულ ვებ გვერდების კატეგორიასთან, რომლებიც წინასწარ შერჩეულია.

მუხლი 10. სისტემების უსაფრთხოება ტესტირებისა და შექმნის პროცესში

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

2. ბიზნესის უწყვეტობის შემუშავებულმა სტრატეგიამ და მისმა ფუნქციონირებამ უნდა უზრუნველყოს სასწავლო უნივერსიტეტის ინფორმაციის დამუშავების პროცესში მოულოდნელი წყვეტის რისკის შემცირება და მოახდინოს მისი დროული აღდგენა.

3. ძირითადი როუტერის მწყობრიდან გამოსვლის შემთხვევაში ხდება სარეზერვო როუტერის ჩართვა, შედეგის დადგომიდან 10 წუთის განმავლობაში.

თავი II -სასაწავლო უნივერსიტეტის სასწავლო პროცესის მართვის ელექტრონული სისტემა

მუხლი 11. სასწავლო პროცესის მართვის ახალი სისტემის დანერგვა და აღწერა

1.სასწავლო უნივერსიტეტის სასწავლო პროცესის მართვის სისტემა რომელიც სრულფასოვნად უნდა დაინერგოს 2018 წელს უზრუნველყოფს სასწავლო უნივერსიტეტის საგანმანათლებლო და ადმინისტრაციულ საქმიანობას არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციას დამუშავებასა და დაცვას.

2. სისტემის ზოგადი ფუქნციები, რომელიც დაინერგება სასწავლო უნივერსიტეტში 2018 წელს:

ა) სასწავლო უნივერსიტეტში სასწავლო პროცესის მართვის ავტომატიზაცია

ბ) ფინანსური მოდულის ავტომატიზაცია

გ) ელექტრონულ საქმის წარმოება

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

4. სისტემის მომხმარებლებია: ა) ადმინისტრაცია ბ) ლექტორი გ) სტუდენტი

მუხლი 12. 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.

მუხლი 13. განვითარების მექანიზმები

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

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

3. სასწავლო უნივერსიტეტი უზრუნველყფს საინფორმაციო რესურსების განვითაერბას, გაუმჯობესებას და პროცესების ოპტიმიზაციისა და მონიტორინგს, როგორც ადმინისტრაციიაში პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუთსორსინგით.