

შპს გეოგლობალ აკადემიის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა

მარნეული

მუხლი 1.

1. წინამდებარე დოკუმენტი განსაზღვრავს შპს გეოგლობალ აკადემიის (შემდგომში - აკადემია) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს აკადემიის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში.
2. წინამდებარე დოკუმენტის შესაბამისი ნაწილების დაცვა სავალდებულოა ყველა იმ პირისთვის, რომლებიც თავის საქმიანობაში იყენებს აკადემიის ინფორმაციულ ტექნოლოგიებსა და რესურსებს.
3. აკადემიის საინფორმაციო ტექნოლოგიების მომხმარებელი (შემდგომში - მომხმარებელი) ვალდებულია დაიცვას საქართველოს კანონმდებლობითა და აკადემიის მიერ დადგენილი მოთხოვნები ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.

მუხლი 2. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

1. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს აკადემიის ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას.
2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროებს წარმოადგენს:
 - ა) აკადემიის ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა;
 - ბ) აკადემიაში 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) აკადემიის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;
- ბ) პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 3. ფიზიკური უსაფრთხოება

1. აკადემიის 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. აკადემია 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. აკადემია ვალდებულია განახორციელოს უსაფრთხოების ინციდენტების იდენტიფიცირება, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას;
2. აკადემიაში ინფორმაციული ტექნოლოგიების სისტემის ფუნქციონირებაზე პასუხისმგებელი პირი პერიოდულად წარმოადგენს ანგარიში და რეკომენდაციები ინფორმაციული უსაფრთხოების ინციდენტების წყაროების (შიდა, გარე) შესახებ.

მუხლი 5. კომუნიკაციებისა და ოპერაციების მართვა

1. აკადემია 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. აკადემია ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება აკადემიის შიგნით და აკადემიის მიზეზით – მის გარეთ;
2. ყველა კრიტიკული სისტემის, აპლიკაციისა და ძირითადი მონაცემის სარეზერვო ასლების აღება ხდება სინქრონულად აკადემიის google drive - ზე.

მუხლი 9. კომპიუტერული ქსელის მართვა

1. აკადემიაში როგორც ფიზიკურ ასევე უკაბელო ქსელში ჩართული კომპიუტერების და მოწყობილობების mac მისამართები რომლებიც განეკუთვნებიან აკადემიის აქტივებს წინასწარ არის გაწერილი როუტერში, რომელიც ანიჭებს წინასწარ შერჩეულ Ip მისამართს.
2. ისეთი მოწყობილობები, რომლებიც არ განეკუთვნებიან აკადემიის აქტივებს და იყენებენ აკადემიის 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.
2. აკადემიამ უნდა უზრუნველყოს 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.

მუხლი 11. სასწავლო პროცესის მართვის სისტემის აღწერა

1. სასწავლო პროცესის მართვის სისტემა უზრუნველყოფს საგანმანათლებლო და ადმინისტრაციულ საქმიანობას, არსებული პროცესების მხარდაჭერას, კომუნიკაციას, ინფორმაციის დამუშავებასა და დაცვას.
2. სისტემის ზოგადი ფუნქციები:
 - ა) სასწავლო პროცესის მართვის ავტომატიზაცია
 - ბ) ფინანსური მოდულის ავტომატიზაცია
 - გ) ელექტრონულ საქმის წარმოება
3. სისტემაში გამოყენებულია კრიპტოგრაფია სადაც დაშიფრულია მომხმარებლების (ადმინისტრაცია, მასწავლებელი, პროფესიული სტუდენტი) პაროლები.
4. სისტემის მომხმარებლებია:
 - ა) ადმინისტრაცია
 - ბ) მასწავლებელი
 - გ) პროფესიული 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 აკადემიის google drive ზე.

მუხლი 13. განვითარების მექანიზმები

1. აკადემიაში არსებული ქსელის ინფრასტრუქტურა მოწყობილია თანამედროვე სტანდარტებით, აკადემია 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. აკადემია უზრუნველყოფს საინფორმაციო რესურსების განვითარებას, გაუმჯობესებას და პროცესების ოპტიმიზაციისა და მონიტორინგს, როგორც ადმინისტრაციაში პროგრამული განვითარების ერთეულის ძალებით, ასევე შესაბამისი მომსახურების აუტსორსინგით.