არასამეწარმეო (არაკომერციული) იურიდიული პირის - საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის რექტორის ბრძანება

№069/01 2018 წლის 5 დეკემბერი ქ. თბილისი

ა(ა)იპ საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის
ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურების დამტკიცების შესახებ

საქართველოს კანონის - „საქართველოს სამოქალაქო კოდექსის“ 35-ე მუხლის, „საგანმანათლებლო დაწესებულებების ავტორიზაციის დებულებისა და საფასურის დამტკიცების შესახებ“ საქართველოს განათლებისა და მეცნიერების მინისტრის 2010 წლის 1 ოქტომბრის №99/ნ ბრძანების, არასამეწარმეო (არაკომერციული) იურიდიული პირის - საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის წესდების მე-4 მუხლის 3 ნაწილის, მე-14 მუხლის პირველი ნაწილის, მე-3 ნაწილის „ბ“, „ე“, „ვ“ და „ლ“ პუნქტისა და მე-4 ნაწილის შესაბამისად, **ვ ბ რ ძ ა ნ ე ბ:**

1. დამტკიცდეს ა(ა)იპ საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები დანართის შესაბამისად.
2. ამ ბრძანების ასლი გამოქვეყნდეს საჯაროდ.
3. ეს ბრძანება თავიანთი კომპეტენციის ფარგლებში შესასრულებლად გადაეგზავნოთ უნივერსიტეტის სტრუქტურულ ერთეულებს/პერსონალს.
4. ბრძანების შესრულებაზე კონტროლს განვახორციელებ პირადად.
5. ბრძანება შეიძლება გასაჩივრდეს საქართველოს კანონმდებლობით დადგენილი წესით.
6. ბრძანება ამოქმედდეს ხელმოწერისთანავე.

პროფესორი, არქიმანდრიტი ადამი
(ვახტანგ ახალაძე)

ა(ა)იპ საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები

მუხლი 1. ზოგადი დებულებები

1. წინამდებარე დოკუმენტი განსაზღვრავს ა(ა)იპ საქართველოს საპატრიარქოს წმინდა თამარ მეფის სახელობის უნივერსიტეტის (შემდგომში - უნივერსიტეტი) ინფორმაციული ტექნოლოგიის მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს უნივერსიტეტის ადმინისტრაციულ საქმიანობასა და საგანმანათლებლო პროცესში.

2. წინამდება წესის შესაბამისი ნაწილების დაცვა სავალდებულოა ყველა იმ პირისთვის, რომლებიც თავის ადმინისტრაციულ, ტექნიკურ, აკადემიურ, სამეცნიერო 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.

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 ელექტრონული საინფორმაციო 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 პირ(ებ)ი 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 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. ბიზნესისუწყვეტობის შემუშავებულმა სტრატეგიამ და მისმა ფუნქციონირებამ უნდა უზრუნველყოს 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.

მუხლი 11. ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა და ხელმისაწვდომობა

1. უნივერსიტეტის ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა მოიცავს:

ა) ტექნიკურ აღჭურვილობას, რომელშიც შედის:

ა.ა) ფიზიკური სერვერები, შესაბამისი პროგრამული უზრუნველყოფით;

ა.ბ) უნივერსიტეტის სტრუქტურულ ერთეულებში მოქმედი კომპიუტერული პროგრამები;

ა.გ) კომპიუტერები/ლეპტოპები, პროექტორი (მათ შორის რამდენიმე ინტერაქტიული) და ქსეროქსის აპარატები;“

ბ) პროგრამულ უზრუნველყოფას (Microsoft Windows, Microsoft office, Adobe (Photoshop, Premiere, Dreamweaver, Illustrator, InDesign), Lira, Sketchup, Autocad, Mathcad, Dev-C++, Oris, Opera, Codex, Web Browser (Chrome, Mozilla) და სხვა, რომლებიც საჭიროების მიხედვით განაწილებულია სტრუქტურულ ერთეულებზე;

გ) ინტერნეტს, რომელზეც წვდომა აქვს უნივერსიტეტის კორპუს(ებ)ში განთავსებულ ყველა კომპიუტერს.

2. უნივერსიტეტის ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა ხელმისაწვდომია უნივერსიტეტის პერსონალისა და სტუდენტებისათვის:

ა) კომპიუტერული ტექნიკა, რომლებიც ჩართულია ინტერნეტში:

ა.ა) ე.წ. „კომპიუტერულ კლასებში“ - სააუდიტორიო მეცადინეობების პერიოდში (საათებში);

ა.ბ) დერეფნებში და ბიბლიოთეკაში განთავსებულ კომპიუტერებზე - ნებისმიერ დროს;

ა.გ) სამუშაო ოთახებში განთავსებულ ტექნიკაზე - შესაბამის პერსონალს;

ბ) უკაბელო ინტერნეტი - ნებისმიერ დროს (არის თავისუფალი, პაროლის გარეშე);

გ) პროექტორები - სააუდიტორიო მეცადინეობების პერიოდში (საათებში), ასევე ნებისმიერ დროს, საჭიროების შემთხვევაში;

დ) ქსეროქსის აპარატები - უნივერსიტეტის სამუშაო საათებში.

მუხლი 12. ინფორმაციული ტექნოლოგიების მართვის პროცედურები

1. უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვას უზრუნველყოფს უნივერსიტეტის საქმისწარმოებისა და ინფორმაციული უზრუნველყოფის სამსახური. აღნიშნული პროცედურები მოიცავს:

ა) სერვერების მართვას:

ა.ა) ტექნიკური უზრუნველყოფა (აწყობა, შემდგომი ექსპლოატაცია);

ა.ბ) პროგრამული უზრუნველყოფა (ინსტალაცია, შემდგომი ექსპლოატაცია).

ბ) კომპიუტერული ტექნიკის მართვას:

ბ.ა) ტექნიკური უზრუნველყოფა (აწყობა, შემდგომი ექსპლოატაცია);

ბ.ბ) პროგრამული უზრუნველყოფა (ინსტალაცია, შემდგომი ექსპლოატაცია).

გ) ინტერნეტის მართვას:

გ.ა) ინტერნეტის მოწოდების ტექნიკური და პროგრამული უზრუნველყოფა;

გ.ბ) ინტერნეტის საჭიროებების მიხედვით შეზღუდვა.

დ) პროგრამული უზრუნველყოფის მართვას: მოძიება; ინსტალაცია და ექსპლოატაცია.

ე) ვებ-გვერდის ადმინისტრირებას: დიზაინის შემუშავებას, ინფორმაციის მიღება-განთავსება და პროგრამული უზრუნველყოფა;

ვ) სამუშაოზე გამოცხადების აღრიცხვის სისტემის (დაშვების აპარატების) მართვას: ტექნიკური კონტროლი, მომხმარებლის დამატება/წაშლა/მომხმარებლის ბარათის აღდგენა (მოხსენებითი ბარათის საფუძველზე);

ზ) ვიდეო-სათვალთვალო სისტემის მართვას: ტექნიკური კონტროლი და კანონმდებლობით დადგენილი წესით შენახვა, ვიდეო-ჩაწერის გამორთვა/ჩართვა, ვიდეო ჩანაწერის ნახვა/სხვა პირთა დაშვება სანახავად (რექტორის სამართლებრივი აქტის საფუძველზე);

თ) ტექნიკური დაზიანების შემთხვევის მართვას: პრობლემის დაზუსტება, დასკვნის მომზადება (საჭიროების შემთხვევაში), საჭირო ნაწილების საწყობიდან გამოტანა, ტექნიკური ხარვეზის გამოსწორება (თუკი მოგვარებადია მიმდინარე ეტაპზე უნივერსიტეტში არსებული რესურსების მეშვეობით);

ი) პროგრამული უზრუნველყოფის დაზიანების შემთხვევის მართვას: პრობლემის დაზუსტება და პროგრამული ხარვეზის გამოსწორება.