თბილისის თავისუფალი უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკა და სახელმძღვანელო პრინციპები

თბილისი, 2024

მუხლი 1. მიზანი

1. წინამდებარე დოკუმენტის მიზანია თბილისის თავისუფალი უნივერსიტეტის (შემდგომში - უნივერსიტეტი) სტუდენტების, კურსდამთავრებულების, პერსონალისა და სხვა პირების შესახებ შეგროვებული პერსონალური მონაცემების დაცვა და აკადემიური მიზნებისათვის გამოყენება.
2. წინამდებარე დოკუმენტი მოიცავს ამ მუხლის პირველ პუნქტში მოცემული პირების პერსონალური მონაცემების დაცვის პრინციპებს, მექანიზმებს, დამუშავებისა და მართვის საკითხებს საქართველოს კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების შესაბამისად.
3. უნივერსიტეტში მონაცემთა დამუშავება ხდება მხოლოდ იმ მოცულობით (მიზნის ადეკვატური და პროპორციული ოდენობით), რომელიც აუცილებელია შესაბამისი კანონიერი მიზნების მისაღწევად.

მუხლი 2. ზოგადი პრინციპები

1. პერსონალურ მონაცემთა დამუშავებისას დაცული უნდა იქნეს შემდეგი ზოგადი პრინციპები:

ა) მონაცემები უნდა დამუშავდეს საქართველოს კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების შესაბამისად.

ბ) მონაცემები უნდა შეგროვდეს/მოპოვებული იქნეს აკადემიური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით.

გ) მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება.

დ) მონაცემები უნდა იყოს ნამდვილი, ზუსტი და, საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე.

ე) მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების აკადემიური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით.

ვ) მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ

უზრუნველყოფს მონაცემთა დაცვას. საუნივერსიტეტო ინფორმაციულ სისტემებზე, სერვერებსა და მონაცემებზე (დოკუმენტები, ფაილები, მონაცემთა ბაზები) მომხმარებლების წვდომა დაფუძნებულია ინფორმაციული უსაფრთხოების უმცირესი პრივილეგიის პრინციპის (PoLP) კონცეფციაზე, რომლის მიხედვითაც მომხმარებელს (მონაცემთა დამმუშავებელს) ეძლევა წვდომის ისეთი შეზღუდული დონე ან უფლებები, რომლებიც საჭიროა მხოლოდ მისი უფლება-მოვალეობებით განსაზღვრული საქმიანობის შესასრულებლად. სისტემაში ყველა დონის მომხმარებლის ავტორიზაცია და მოქმედებები აღირიცხება და კონტროლდება.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ზოგადი პრინციპების გარდა, მონაცემთა დამუშავება შესაძლებელია ეფუძნებოდეს, მათ შორის:

2.1. მონაცემთა სუბიექტის მოთხოვნას;

2.2. მონაცემთა სუბიექტის თანხმობას (ზეპირ ან წერილობით თანხმობას);

2.3. კანონმდებლობის საფუძველზე უნივერსიტეტისათვის დაკისრებულ ვალდებულებებს;

2.4. უნივერსიტეტის აღმატებულ ლეგიტიმურ ინტერესებს;

2.5. საჯარო ინტერესებს;

2.6. შრომითი ურთიერთობებს.

მუხლი 3. აკადემიური მიზანი

1. პერსონალურ მონაცემთა დამუშავება ხდება საქართველოს კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების საფუძველზე, უნივერსიტეტის მიერ ადმინისტრაციული/სასწავლო/სამეცნიერო პროცესისა და საქმიანობის წარმართვისთვის კონკრეტული და მკაფიო აკადემიური მიზნების უზრუნველსაყოფად.

2. უნივერსიტეტის აკადემიური ბუნებიდან გამომდინარე, აკადემიურ მიზანს წარმოადგენს ადმინისტრაციული/სასწავლო/სამეცნიერო პროცესის და საქმიანობის უზრუნველყოფის მიზნით განხორციელებული ქმედებები, მათ შორის:

ა) საგანმანათლებლო პროგრამებისა და კვლევის განვითარება და მიწოდება;

ბ) სტუდენტების მოზიდვის მექანიზმები და მხარდაჭერის სერვისები;

გ) პერსონალის შერჩევისა და მხარდაჭერის მექანიზმები;

დ) სტუდენტების აკადემიური მოსწრების მონიტორინგი;

ე) საგამოცდო მიზნებისათვის პიროვნების იდენტიფიკაცია;

ვ) ეთიკის სტანდარტებით გათვალისწინებული პრინციპების დაცვა, მათ შორის, პლაგიარიზმსა და აკადემიურ თაღლითობასთან ბრძოლის მექანიზმები;

ზ) სტუდენტებისათვის საქართველოს კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების შესაბამისად კვალიფიკაციის მინიჭება;

თ) უნივერსიტეტის შიდა მარეგულირებელი აქტების აღსრულების უზრუნველყოფა;
ი) კურსდამთავრებულთა კარიერული განვითარება და მხარდაჭერა.

მუხლი 4. შრომითი ურთიერთობებიდან გამომდინარე პერსონალური მონაცემები

საქართველოს შრომის კოდექსის, უმაღლესი განათლების კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების საფუძველზე, უნივერსიტეტი პერსონალის შესახებ ამუშავებს პერსონალური ინფორმაციის შემცველ მონაცემებს, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს, რაც აკადემიური მიზნების ეფექტიანად განხორციელებისა და სტუდენტთა ინტერესების დაცვითაა განპირობებული.

მუხლი 5. აბიტურიენტების/აპლიკანტების, სტუდენტებისა და კურსდამთავრებულების შესახებ პერსონალური მონაცემები

უნივერსიტეტის საწესდებო ამოცანების განსახორციელებლად, აკადემიური მიზნებიდან გამომდინარე უმაღლესი განათლების კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების საფუძველზე, უნივერსიტეტი ამუშავებს აბიტურიენტების/აპლიკანტების, სტუდენტებისა და კურსდამთავრებულების შესახებ პერსონალურ მონაცემებს, მათ შორის, განსაკუთრებული კატეგორიის მონაცემებს, რაც სტუდენტის აკადემიური მიზნებითა და ინტერესებითაა განპირობებული.

მუხლი 6. განათლების მართვის საინფორმაციო სისტემა

1. უნივერსიტეტი იყენებს განათლების მართვის ინფორმაციულ სისტემას - EMIS (emis.campus.edu.ge). აღნიშნული ელექტრონული სისტემა უზრუნველყოფს: სტუდენტების შესახებ ინფორმაციის აღრიცხვას, მათი მიღების, მობილობის და სტატუსის ცვლილების პროცესებს; სასწავლო კურსების აღრიცხვას; კურიკულუმებისა და სემესტრული გეგმების ფორმირებას; სილაბუსებზე წვდომას; უწყისებისა და შეფასებების აღრიცხვას; მაინორების, კონცენტრაციებისა და არჩევით სასწავლო კურსებზე რეგისტრაციას წინაპირობების დაცვით; სტუდენტების საფასურის აღრიცხვას/დარიცხვას და მისი ანგარიშსწორების პროცესს; ბიბლიოთეკის ელექტრონული კატალოგის ხელმისაწვდომობას და ა.შ.
2. EMIS გააჩნია როლების განაწილებული ფუნქციონალი და უნივერსიტეტის მიერ ავტორიზებულ თანამშრომლებს აქვთ წვდომა მათთვის განკუთვნილ ინფორმაციასა და პროცესზე იმგვარად, რომ დაცული იყოს ინფორმაციის სიზუსტე, მთლიანობა და ანონიმურობა. აღნიშნული სისტემა წარმოადგენს "ღრუბლოვან სერვისს" (Cloud Service) და ხორციელდება სისტემის მონაცემთა ბაზის ყოველდღიური რეზერვირება.
3. EMIS-ზე განთავსებული პერსონალური მონაცემების მოპოვება ხორციელდება:

ა) სსიპ - შეფასებისა და გამოცდების ეროვნული ცენტრის მიერ მოწოდებული ჩარიცხვების სიის მეშვეობით;
ბ) პირველადი რეგისტრაციის ეტაპზე სტუდენტების შესახებ პერსონალური ინფორმაციის მოპოვების გზით, ელექტრონული რეგისტრაციის კითხვარზე პასუხების მეშვეობით;
გ) უნივერსიტეტის უფლებამოსილი პირების მიერ სასწავლო და სარეგისტრაციო პროცესში სტუდენტთან დაკავშირებული ინფორმაციის შეტანითა და განახლებით EMIS-ზე.

4. EMIS-ის მეშვეობით სტუდენტის პერსონალური მონაცემების დამუშავება ხორციელდება შემდეგი ფორმებით: შეგროვება, მოპოვება, მათზე წვდომა, ფოტოგადაღება, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა, აგრეთვე, მონაცემთა გამჟღავნება მათი გადაცემით.

5. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ვ“ პუნქტისა და მე-5 მუხლის „ა“, „ბ“, „გ“, „დ“, „კ“ ქვეპუნქტების საფუძველზე, აკადემიური მიზნით, EMIS-ის მეშვეობით მუშავდება სტუდენტის შესახებ შემდეგი სახის პერსონალური მონაცემები: პირადი მონაცემები, საგანმანათლებლო ინფორმაცია, სასწავლო ბარათი, ნიშნების ფურცელი.

6. უნივერსიტეტი იყენებს დამუშავებაზე უფლებამოსილი პირის მომსახურებას ტექნიკური მხარდაჭერის პროცესში. ტექნიკური მხარდაჭერა გულისხმობს შემდეგ მომსახურებას: სტუდენტთა ერთიანი ელექტრონული რეესტრის შექმნა-წარმოება, სასწავლო პროცესის მართვის ელექტრონული სერვისების გამართული ტექნიკური უზრუნველყოფა, სატელეფონო, ფიზიკური და ონლაინ-კონსულტაცია მართვის სისტემის გამართულ ფუნქციონირებასთან დაკავშირებით, მონაცემთა ბაზის რეზერვაცია და უსაფრთხოება, სისტემის სხვადასხვა მოდულის ფუნქციური მოდიფიცირება, სრულყოფა, გამართვა, განახლება. დამუშავებაზე უფლებამოსილ პირთან ურთიერთობა რეგულირდება მხარეებს შორის გაფორმებული ხელშეკრულებით.

7. EMIS-ის მეშვეობით დამუშავებული პერსონალური მონაცემების მესამე პირებისთვის გადაცემის ფაქტები აღირიცხება და კომუნიკაცია ხორციელდება შესაბამისი პირის მიერ ელექტრონული ფოსტის მეშვეობით.

8. EMIS-ში არსებული მონაცემების (სტუდენტის პირადი მონაცემები, საგანმანათლებლო ინფორმაცია, სასწავლო ბარათი, ნიშნების ფურცელი; ლექტორების პირადი მონაცემები და აკადემიური გამოცდილება; ადმინისტრატორების პირადი მონაცემები) და შესაბამისი ავტორიზებული პირების მიერ EMIS-ის მეშვეობით განხორციელებული მოქმედებების შენახვის ვადები, ასევე, EMIS სისტემისა და მასში განხორციელებული მოქმედებების, მონაცემთა ბაზების სარეზერვო ასლების შენახვის ვადები განისაზღვრება რექტორის ბრძანებით.

9. EMIS-ზე მონაცემთა ბაზის პერსონალურ მონაცემებზე წვდომის მქონე, ასევე, EMIS-ის სერვერების ადმინისტრირებასა ან/და ტექნიკური მხარდაჭერაზე ავტორიზებული/უფლებამოსილი პირები განისაზღვრება რექტორის ბრძანებით.
10. EMIS-ზე წვდომის უფლების მქონე ავტორიზებულ პირს გააჩნია ინდივიდუალური მომხმარებლის სახელი და პაროლი. პორტალზე ავტორიზაცია ხორციელდება Google Workspace ანგარიშის საშუალებით, რომელზეც პაროლის მინიმალური მოცულობა არის 8 სიმბოლო, ხოლო პაროლის სავალდებულო ცვლილება ხორციელდება წელიწადში მინიმუმ ერთხელ.
11. პერსონალური მონაცემების დამუშავების პროცესში ჩართული პირები ვალდებული არიან emis.campus.edu.ge-ზე სამსახურებრივი მოვალეობის შესრულების დროს დამუშავებული პერსონალური მონაცემები, რომლებიც ინახება მათ სამუშაო (სამსახურებრივ/პირად) პერსონალურ კომპიუტერებზე ან სხვა ნებისმიერ მოწყობილობაზე, წაშალონ/გაანადგურონ შრომითი ხელშეკრულების შეწყვეტისთანავე უნივერსიტეტის საინფორმაციო ტექნოლოგიების სამსახურის ავტორიზებული თანამშრომლის მეთვალყურეობის ქვეშ.
12. EMIS-ის მეშვეობით პერსონალური მონაცემების მიმართ შეიძლება განხორციელდეს მოქმედებები, რომლებიც აღირიცხება და რომელთა ტიპი და შენახვის ვადები განისაზღვრება რექტორის ბრძანებით.

მუხლი 7. მონაცემთა შენახვა

1. პერსონალური მონაცემები ინახება როგორც ელექტრონული, ასევე მატერიალური ფორმით განსაზღვრული ვადით, უვადოდ და საარქივო მიზნებისათვის.
2. მონაცემთა შენახვის ვადები განისაზღვრება რექტორის ბრძანებით.
3. მატერიალური სახით არსებული პერსონალური მონაცემები ინახება სპეციალურად გამოყოფილ კონტროლირებადი დაშვების დაცულ ადგილას.

მუხლი 8. დისტანციურად მუშაობისას მონაცემთა დამუშავება

1. დისტანციური მუშაობის განხორციელებისას უნივერსიტეტი, როგორც საგანმანათლებლო დაწესებულება უფლებამოსილია დისტანციური შეხვედრების გამართვისათვის გამოიყენოს ელექტრონული კომუნიკაციის სისტემები.
2. დისტანციურად მუშაობისას უნივერსიტეტის პერსონალს შეუძლია გამოიყენოს საკუთარი კომპიუტერი, რომელზეც სხვა პირებს არ უნდა ჰქონდეთ დაშვება.
3. მონაცემთა უსაფრთხოების მიზნით, უნივერსიტეტი უზრუნველყოფს პერსონალის კუთვნილ კომპიუტერებზე პროგრამული უზრუნველყოფისა და ოპერაციული სისტემების ინსტალაციას, გამართვასა და განახლებას.

4. სავალდებულოა, როგორც სამუშაო, ისე პერსონალის კუთვნილ კომპიუტერში შესვლის პაროლის დაყენება. აგრეთვე, იმ ელექტრონულ სისტემებში შესვლისთვის, რომელზეც წვდომა ინდივიდუალური მომხმარებლის სახელით არის შესაძლებელი, გამოიყენება რთული და კომპლექსური პაროლი (რომელიც შეიცავს არანაკლებ 8 სიმბოლოს). უნივერსიტეტის შიდა ელექტრონულ რესურსებთან წვდომისათვის გამოიყენება მხოლოდ დაშიფრული VPN კავშირის საშუალებები.
5. რეგულარულად მიმდინარეობს მონაცემების სარეზერვო ასლების შექმნა, რომლის შენახვის ვადები განისაზღვრება რექტორის ბრძანებით.
6. უნივერსიტეტი პერსონალისთვის ქმნის უკაბელო ქსელური კავშირისთვის საჭირო წვდომის ინდივიდუალურ პარამეტრებს. უკაბელო ქსელურ მოწყობილობასთან დაკავშირების გამოიყენება კომპლექსური სახის პაროლი, არანაკლებ 9 სიმბოლოსგან შემდგარი; უკაბელო ქსელური კავშირისათვის გამოიყენება შიფრაციის თანამედროვე მეთოდები. არსებობს უკაბელო ქსელურ კავშირთან მომხმარებლების ღია (ვიზიტორებისა და სტუდენტებისათვის) და დახურული (პერსონალისათვის) წვდომა. აღნიშნული ქსელების მომხმარებლები ერთმანეთისაგან იზოლირებულია. ქსელზე დაშვება აღირიცხება და ინახება 1 თვის ვადით.

მუხლი 9. მონაცემებზე წვდომის უფლების მქონე სუბიექტები

უნივერსიტეტის წინაშე მდგარი აკადემიური მიზნებისა და მისი ფუნქციონირების ეფექტიანობის უზრუნველსაყოფად, მონაცემებზე წვდომა საკუთარი კომპეტენციის ფარგლებში შესაძლებელია ჰქონდეს: რექტორს, პრორექტორებს, კანცლერს, სარეგისტრაციო და სასწავლო პროცესის მართვის სამსახურს, ხარისხის უზრუნველყოფის სამსახურს, ადამიანური რესურსების მენეჯერს, საინფორმაციო ტექნოლოგიების სამსახურს, ფინანსურ ანალიტიკოსებს, სტუდენტებსა და აბიტურიენტებთან ურთიერთობის სამსახურს, სამეცნიერო საქმიანობის კოორდინატორს, აკადემიური პერსონალის პროფესიული განვითარების მენეჯერს, პროფესიული პროგრამების მენეჯერს, კანცელარიასა და არქივს, იურიდიულ სამსახურს, საზოგადოებასთან ურთიერთობისა და მარკეტინგის მენეჯერს, გამომცემლობისა და ივენთების მენეჯერს, მედია სტუდიას, საგამოცდო ცენტრს, საერთაშორისო ურთიერთობების მენეჯერს, ბიბლიოთეკას, უნივერსიტეტის სკოლებსა და კვლევით ცენტრებს, ლექტორებს.

მუხლი 10. ვიდეოკონტროლის განხორციელება

1. სტუდენტებისა და სხვა პირთა უსაფრთხოებისა და წესრიგის უზრუნველყოფის მიზნით უნივერსიტეტის შენობის შიდა და გარე პერიმეტრზე მიმდინარეობს ვიდეოკონტროლი.

2. აკადემიურ თაღლითობასთან ეფექტიანი ბრძოლისა და სტუდენტთა შედეგების ობიექტური შეფასების უზრუნველსაყოფად, საგამოცდო ცენტრში მიმდინარეობს ვიდეოკონტროლი. ვიდეოჩანაწერი საშუალოდ 1 თვის განმავლობაში ინახება.
3. ღია სამუშაო სივრცეებში უსაფრთხოების უზრუნველყოფის მიზნით მიმდინარეობს ვიდეოკონტროლი. ვიდეოჩანაწერი საშუალოდ 1 თვის განმავლობაში ინახება.
4. უნივერსიტეტის ტერიტორიაზე წარმოებული ვიდეოკონტროლის შესახებ გამაფრთხილებელი ნიშნები განთავსებულია თვალსაჩინო ადგილებში.
5. უნივერსიტეტის ვიდეოკონტროლის სისტემაზე წვდომას ახორციელებს: დაცვის სამსახური, კანცლერი და საინფორმაციო ტექნოლოგიების სამსახურის შესაბამისი უფლებამოსილი თანამშრომლები.
6. უნივერსიტეტში ვიდეოკონტროლი ხორციელდება მხოლოდ ამ მუხლით გათვალისწინებული მიზნებით.

მუხლი 11. შენობაში შესვლისა და გასვლის აღრიცხვა

1. უსაფრთხოებისა და წესრიგის უზრუნველყოფის მიზნით, უნივერსიტეტის გარე და შიდა პერიმეტრზე შესვლისა და გასვლის აღრიცხვა (თარიღი, დრო, მდებარეობა), ასევე, სხვადასხვა სივრცეში დაშვების მართვა, ხორციელდება დაშვების კონტროლის ელექტრონული სისტემის გამოყენებით.
2. აღრიცხვა ხორციელდება ელექტრონული ბარათების გამოყენებით.
3. უნივერსიტეტი, კონტროლის განხორციელების მიზნით, აგროვებს შემდეგ მონაცემებს: სახელი, გვარი, პირადი ნომერი, შესვლისა და გასვლის თარიღები, დრო და ლოკაცია.
4. უნივერსიტეტის გარე და შიდა პერიმეტრზე შესვლისა და გასვლის აღრიცხვის მიზნით დაშვების კონტროლის ელექტრონულ სისტემაზე წვდომას ახორციელებს საინფორმაციო ტექნოლოგიების სამსახური.

მუხლი 12. ელექტრონული ფოსტისა და ტელეფონის ნომრის გამოყენება

აკადემიური მიზნებიდან გამომდინარე ეფექტიანი და სწრაფი კომუნიკაციისათვის, უნივერსიტეტი ამუშავებს პერსონალის, სტუდენტებისა და კურსდამთავრებულების ელექტრონულ ფოსტებსა და ტელეფონის ნომრებს.

მუხლი 13. ინფორმაციული ტექნოლოგიების სერვისების უწყვეტად მუშაობის უზრუნველყოფა

1. შიდა ქსელური ინფრასტრუქტურის კრიტიკული კომპონენტები, რომლებიც უზრუნველყოფენ ქსელური სერვისების მიწოდებას აქტიურად დუბლირებულია, ანუ მუშაობს პარალელურად. ერთ-ერთის დაზიანების შემთხვევაში სისტემა უწყვეტად

აგრძელებს მუშაობას მეორე მოწყობილობით. ნაკლებად კრიტიკული მოწყობილობების ჩანაცვლება კი ხდება საინფორმაციო ტექნოლოგიების სამსახურის მუდმივად განახლებადი, კონტროლირებადი მარაგიდან საკუთარი ძალებით, დამოუკიდებლად. გარდა ამისა, სისტემატურად ხორციელდება ძირითადი ქსელური აპარატურის კონფიგურაციის სარეზერვო ასლების შენახვა. დაზიანებული მოწყობილობების ახლით ჩანაცვლებისას აღნიშნული მონაცემების გამოყენება ამცირებს სერვისის წყვეტის დროს.

2. ქსელური ინფრასტრუქტურის ყველა კვანძის უწყვეტი მუშაობა უზრუნველყოფილია უწყვეტი კვების წყაროებითა და გენერატორით.

3. ინფორმაციული ტექნოლოგიებთან დაკავშირებული სავარაუდო რისკი შესაძლებელია იყოს ინფორმაციული სერვისების წყვეტა როგორც აპარატურული, ასევე პროგრამული უზრუნველყოფის დაზიანების ან კიბერშეტევის გამო. უნივერსიტეტში არსებული ინფორმაციული სერვისები იყოფა ორ - შიდა და გარე კატეგორიად:

ა) შიდა - საშუალო და ზოგიერთი მაღალი რისკის კატეგორიის სერვისების უზრუნველყოფა ხდება უნივერსიტეტის ტექნიკური ინფრასტრუქტურისა და საინფორმაციო ტექნოლოგიების სამსახურის საშუალებით;

ბ) გარე - მაღალი და ზოგიერთი საშუალო რისკის გარე სერვისების უზრუნველყოფა ხდება სხვა ორგანიზაციების მიერ, ხელშეკრულების საფუძველზე.

4. შიდა სერვისების უწყვეტად მუშაობისთვის უნივერსიტეტის და საინფორმაციო ტექნოლოგიების სამსახურის მიერ უზრუნველყოფილია:

ა) სერვერული აპარატურის ფიზიკური დუბლირება;

ბ) სერვერულ მოწყობილობებზე დისკების დუბლირება;

გ) მონაცემთა სანახებზე დისკების დუბლირება და რეზერვირება;

დ) ოპერაციული სისტემების სისტემატური რეზერვირება;

ე) სერვერების ქსელური აპარატურის დუბლირება;

ვ) სერვერების ქსელური უსაფრთხოება;

ზ) ქსელური აპარატურის კონფიგურაციების რეზერვირება;

თ) სერვერული აპარატურის გაგრილება და ამ სისტემების დუბლირება;

ი) სერვერული აპარატურის სახანძრო მონიტორინგი;

კ) სერვერული აპარატურის უწყვეტი ელ. მომარაგებით უზრუნველყოფა;

ლ) სერვერული სისტემების აპარატურული და პროგრამული განახლება;

მ) ოპერაციული სისტემების განახლება;

ო) პროგრამული სერვისების პროგრამული უზრუნველყოფის განახლება.

5. გარე კატეგორიის სერვისების უწყვეტად ფუნქციონირებისთვის მომწოდებლების ხელშეკრულებებსა თუ მომსახურების შეთანხმების პირობებში გათვალისწინებულია ზემოთ ჩამოთვლილი სერვისების არსებობა სერვისის შესაბამისობით.

6. პრობლემის პრევენციისთვის საინფორმაციო ტექნოლოგიების სამსახურის მიერ ხორციელდება ყველა შიდა სერვისის, სერვერის, ოპერაციული სისტემისა და, ასევე, გარე სერვისების ავტომატიზებული მონიტორინგი 24-საათიან რეჟიმში, რომლის საშუალებითაც ხდება ინციდენტების პრევენცია ან მათზე მყისიერი რეაგირება. შესაბამისად, ნებისმიერი ინციდენტის შემთხვევაში ხდება მონაცემთა აღდგენა.

7. უნივერსიტეტი ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები, ინციდენტის აღმოჩენიდან არა უგვიანეს 72 საათისა, მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებ სავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

8. უნივერსიტეტი ვალდებულია, აღრიცხოს მონაცემთა დამუშავებასთან დაკავშირებული, მათ შორის, ინციდენტის შესახებ ინფორმაცია. უნივერსიტეტი აღნიშნულ ვალდებულებას ასრულებს ყველა აღმოჩენილ ინციდენტთან დაკავშირებით, მიუხედავად იმისა, ექვემდებარება თუ არა ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის ან/და მონაცემთა სუბიექტისთვის შეტყობინებას.

9. ინციდენტის სახეებია:

ა) კონფიდენციალურობის დარღვევა – პერსონალური მონაცემების უნებართვო გამჟღავნება ან წვდომა;

ბ) მთლიანობის დარღვევა – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა;

გ) ხელმისაწვდომობის დარღვევა – პერსონალურ მონაცემებზე წვდომის დაკარგვა, შეზღუდვა, მონაცემების განადგურება ან წაშლა.

10. ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი საფრთხის შექმნის სიმძიმის განსაზღვრის მიზნებისთვის, უნივერსიტეტმა უნდა გაითვალისწინოს შემდეგი გარემოებები:

ა) რა სახის ინციდენტს აქვს ადგილი (პერსონალურ მონაცემთა კონფიდენციალურობის, მთლიანობის თუ ხელმისაწვდომობის დარღვევას);

ბ) იმ პერსონალური მონაცემების კატეგორია, რომლებზეც გავლენას ახდენს ინციდენტი;

გ) ეხება თუ არა ინციდენტი არასრულწლოვანის, შეზღუდული შესაძლებლობის მქონე პირისა ან სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტის პერსონალურ მონაცემებს;

დ) ინციდენტის შედეგად მონაცემთა სუბიექტის მესამე პირთა მიერ იდენტიფიცირების შესაძლებლობის ხარისხი;

ე) დამუშავებისთვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი, რასაც შესაძლოა ახლდეს მომეტებული საფრთხე;
ვ) ინციდენტის მასშტაბი, მონაცემთა სუბიექტის ან/და პერსონალური მონაცემის რაოდენობის ან/და მოცულობის თვალსაზრისით;
ზ) სხვა ისეთი გარემოება, რამაც შესაძლოა არსებითი გავლენა მოახდინოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შექმნის ალბათობის სიმძიმეზე.

მუხლი 14. პერსონალისა და სტუდენტების პასუხისმგებლობა

1. უნივერსიტეტში დასაქმებული პირები ვალდებულნი არიან დაიცვან უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკისა და სახელმძღვანელო პრინციპების დოკუმენტი, როგორც მათი ხელშეკრულების განუყოფელი ნაწილი.
2. უნივერსიტეტში დასაქმებულ პირებს ეკრძალებათ პერსონალური მონაცემების შემცველი დოკუმენტებისა და ფაილების უყურადღებოდ დატოვება.
3. უნივერსიტეტის პერსონალი ვალდებულია არ გაამჟღავნოს და არ გადასცეს პერსონალური მონაცემები სხვა პირებს. პერსონალური მონაცემების დაცვის ვალდებულება გააჩნიათ იმ შემთხვევაშიც, თუ ისინი აღარ იქნებიან დასაქმებულნი უნივერსიტეტში.
4. პერსონალური მონაცემების დამუშავების შესახებ დადგენილი წესების დარღვევა არის უნივერსიტეტის პერსონალის მიმართ დისციპლინური დევნის დაწყების საფუძველი და შესაძლოა გახდეს შრომითი ურთიერთობების შეწყვეტის საფუძველი.
5. სტუდენტები ვალდებულნი არიან დაიცვან უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკისა და სახელმძღვანელო პრინციპების დოკუმენტი.
6. სტუდენტები ვალდებულნი არიან დროულად შეატყობინონ უნივერსიტეტს თავიანთი პერსონალური მონაცემების ცვლილების შესახებ.
7. უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკითა და სახელმძღვანელო პრინციპებით დადგენილი წესების დარღვევა არის სტუდენტის მიმართ დისციპლინური დევნის დაწყების საფუძველი.