დამტკიცებულია:

სსიპ - თბილისის სახელმწიფო სამედიცინო უნიერსიტეტის

რექტორის 2024 წლის 4 ნოემბრის

#1410546 ბრძანებით

სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკა

მუხლი 1. პოლიტიკის ცნება და მიზანი

1.სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის (შემდგომში - უნივერსიტეტი“) პერსონალურ მონაცემთა დაცვის პოლიტიკა (შემდგომში- პოლიტიკა) განსაზღვრავს უნივერსიტეტში მონაცემების დამუშავების წესებსა და პროცედურებს, მონაცემთა უსაფრთოების დაცვის ღონისძიებებს.

მუხლი 2. პერსონალურ მონაცემთა დაცვის პოლიტიკის მოქმედების სფერო

1.პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტის მოქმედება ვრცელდება უნივერსიტეტში დასაქმებულ პირებზე, უნივერსიტეტის სტუდენტებზე და ასევე სხვა პირებზე, რომლებიც უნივერსიტეტის სახელით ახორციელებენ თავიანთ უფლებამოსილებას.

2.პერსონალურ მონაცემთა დაცვის პოლიტიკის მიზანს წარმოადგენს გამჭირვალე გახადოს უნივერსიტეტის მიზნებისა და საქმიანობის გათვალისწინებით შეგროვებული პერსონალური მონაცემების დაცვისა და დამუშავების წესები და პროცედურები, კანონმდებლობის შესაბამისად უზრუნველყოს დამუშავების პროცესის წარმართვა, ფიზიკური პირის უფლებების დაცვა და დამუშავების პროცესი.

3. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი ახორციელებს სტუდენტების, კურსდამთავრებულების, პერსონალისა და სხვა პირების შესახებ შეგროვებული პერსონალური მონაცემების დაცვას და აკადემიური მიზნებისათვის მათ გამოყენებას.

მუხლი 3. ტერმინთა განმარტება.

1. წინამდებარე დოკუმენტში გამოყენებული ტერმინები მხოლოდ აღწერილობითი ხასიათისაა და განმარტებულია უნივერსიტეტის სამუშაო სპეციფიკიდან გამომდინარე. განმარტებები შესაბამისობაშია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან და მათი ინტერპრეტირება კანონის საწინააღმდეგოდ დაუშვებელია:

1.1. პერსონალური მონაცემი (შემდგომში - მონაცემი) - ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს და გამოიყენება უნივერსიტეტის საქმიანობის მიზნებიდან გამომდინარე. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული, რასობრივი, სოციალური ან სხვა ნიშნებით;

1.2. მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი, რომლის შესახებ არსებული მონაცემი გამოიყენება უნივერსიტეტის მიერ საკუთარი მიზნებიდან გამომდინარე. ფიზიკური პირი შესაძლებელია იყოს იდენტიფიცირებული ან იდენტიფიცირებადი;

1.3. მონაცემთა დამმუშავებელი - უნივერსიტეტი არის მონაცემთა დამმუშავებელი, რომელიც განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, მეთოდებს, ფორმებს, ორგანიზაციული და ტექნიკური უსაფრთხოების ზომებს, ასევე, მონაცემთა სუბიექტის უფლებების რეალიზაციის გზებს;

1.4. ფაილური სისტემა – მონაცემთა სტრუქტურიზებული წყობა, რომელშიც ისინი დალაგებული და ხელმისაწვდომია კონკრეტული კრიტერიუმის მიხედვით;

1.5. ფაილური სისტემის კატალოგი – ფაილური სისტემის სტრუქტურისა და შინაარსის დეტალური აღწერილობა;

მუხლი 4. მონაცემთა დაცვის პრინციპები

1. უნივერსიტეტის მიერ პერსონალური მონაცემების დამუშავების პროცესის კანონიერად წარმართვისათვის, კანონიერი საფუძვლის გარდა აუცილებელია მონაცემთა დამუშავების პრინციპების დაცვაც, შესაბამისად უნივერსიტეტი პერსონალურ მონაცემთა დამუშავებისას უზრუნველყოფს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული შემდეგი პრინციპების დაცვას:

1.1. სამართლიანობა, კანონიერება, გამჭირვალობა და ღირსების დაცვა - მონაცემები უნდა დამუშავდეს სამართლიანად, კანონიერად, მონაცემთა სუბიექტისათვის გამჭირვალედ და ადამიანის ღირსების შეულახავად (მონაცემები უნდა დამუშავდეს საქართველოს კანონმდებლობისა და უნივერსიტეტის შიდა მარეგულირებელი აქტების შესაბამისად);

1.2. კონკრეტული კანონიერი მიზნის არსებობის აუცილებლობა - ზუსტად უნდა განისაზღვროს, თუ რა მიზნით ხდება პერსონალური მონაცემების დამუშავება (მონაცემები უნდა შეგროვდეს/მოპოვებული იქნეს აკადემიური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით);

1.3. პროპორციულობა - მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება (მინიმიზაცია);

1.4. ნამდვილობა და სიზუსტე - მონაცემები უნდა იყოს ნამდვილი, ზუსტი და საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით,

არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე;

1.5. 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;

1.6. 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. ზემოაღნიშნული პრინციპების გარდა, უნივერსიტეტი იცავს დამუშავების კანონით გათვალისწინებულ საფუძვლებს, როგორც არასენსიტიური, ისე განსაკუთრებული კატეგორიის მონაცემისათვის, კერძოდ დამუშავება შესაძლებელია, მათ შორის ეფუძნებოდეს:

2.1. მონაცემთა სუბიექტის თანხმობას - ზეპირი ან წერილობითი თანხმობა. იმისათვის, რომ პერსონალური მონაცემების დამუშავებას საფუძვლად დაედოს მონაცემთა სუბიექტის თანხმობა, აუცილებელია რომ ეს თანხმობა: იყოს ნებაყოფლობითი; გამოხატული იყოს წინასწარ, მონაცემთა დამუშავებამდე; გამოხატული იყოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის მიღების შემდეგ; გამოხატული იყოს კონკრეტული მკაფიოდ განსაზღვრული კანონიერი მიზნით მონაცემთა დამუშავებაზე; გამოიხატოს ისეთი საშუალებით, რომლითაც ნათლად დგინდება მონაცემთა სუბიექტის ნება;

2.2. კანონმდებლობით გათვალისწინებულ მოთხოვნებს, რისი შესრულების ვალდებულებაც აკისრია უნივერსიტეტს (მათ შორის, განათლების სფეროს მარეგულირებელი კანონქვემდებარე აქტებით განსაზღვრული ვალდებულებები);

2.3. უნივერსიტეტის აღმატებულ ლეგიტიმურ ინტერესებს;

2.4. საჯარო ინტერესებს;

2.5. შრომითი ვალდებულებების, შრომითი ურთიერთობებისა და დასაქმების თაობაზე გადაწყვეტილების მიღებას.

მუხლი 5. უნივერსიტეტის საქმიანობის ფარგლებში დამუშავებული მონაცემები

1.უნივერსიტეტი ამუშავებს სტუდენტის, აკადემიური და ადმინისტრაციული პერსონალის ასევე სხვა პირის პერსონალურ მონაცემებს, რომლის ჩამონათვალი ვადების მითითებით განთავსებულია დანართი 1-ის სახით.

2. უნივერსიტეტის ამუშავებს შემდეგ მონაცემებს:

2.1 ადმინისტრაციული პერსონალის, აკადემიური პერსონალის , მოწვეული პერსონალის და დამხმარე პერსონალის შესახებ - სახელი, გვარი, ფოტოსურათი, დაბადების თარიღი, ასაკი, სქესი, მისამართი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის ასლი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, მართვის მოწმობის ასლი, ავტობიოგრაფია, რეზიუმე (CV), განათლების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, სამუშაო გამოცდილების შესახებ ინფორმაცია, შენობაში შესვლისა და შენობიდან გასვლის დრო, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, საბანკო ანგარიშის ნომერი, დაკავებული პოზიცია (თანამდებობა), ანაზღაურების შესახებ ინფორმაცია, ინფორმაცია ნასამართლობის შესახებ, ინფორმაცია სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის ნასამართლობის შესახებ, ინფორმაცია ჯანმრთელობის მდგომარეობის შესახებ (ფორმა100);

2.2. პოტენციური დასაქმებულის შესახებ - სახელი, გვარი, ავტობიოგრაფია, რეზიუმე (CV), დიპლომის ასლი ან განათლების დამადასტურებელი მოწმობა, სამუშაო გამოცდილების შესახებ ინფორმაცია, უცხო ენის ცოდნის შესახებ ინფორმაცია, კომპიუტერული პროგრამების ცოდნის შესახებ ინფორმაცია, შენობაში შესვლისა და შენობიდან გასვლის დრო, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი;

2.3. სტუდენტის შესახებ - სახელი, გვარი, პირადი ნომერი, პირადობის დამადასტურებელი დოკუმენტის სერია და ნომერი, პირადობის დამადასტურებელი დოკუმენტის გაცემის ვადა, ფოტოსურათი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, დაბადების თარიღი, უცხო ენის ცოდნა, სქესი, განათლების შესახებ ინფორმაცია, მოქალაქეობა, სამხედრო ვალდებულების შესახებ ინფორმაცია, სტუდენტის სასწავლო ბარათის ასლი ან მისი ამონაწერი, სტუდენტის სტატუსის განმსაზღვრელი ყველა სამართლებრივი აქტის/აქტები (ჩარიცხვის ბრძანება, სტატუსის შეჩერება, აღდგენა, სტიპენდიის მინიჭება), კანონმდებლობის შესაბამისად სწავლების უფლების მინიჭებაზე საქართველოს განათლებისა, მეცნიერების და ახალგაზრდობის საქმეთა სამინისტროს ბრძანების ასლი, შენობაში შესვლისა და შენობიდან გასვლის დრო;

2.4. ვიზიტორის შესახებ - სახელი, გვარი, შენობიდან შესვლისა და შენობიდან გასვლის დრო, ავტომობილის სახელმწიფო სარეგისტრაციო ნომერი.

3. უნივერსიტეტი, იმ პერსონალურ მონაცემებს, რომლის დამუშავების საფუძვლები არ არის კანონით განსაზღვრული ამუშავებს მონაცემთა სუბიექტის თანხმობით.

4. უნივერსიტეტი უზრუნველყოფს პერსონალური მონაცემების დამუშავების შესახებ დასაქმებულისა და სტუდენტის ინფორმირებას ხელშეკრულებისა და მონაცემთა დაცვის პოლიტიკის დოკუმენტის მეშვეობით.

5. კანონმდებლობის თანახმად, პანდემიის, ეპიდემიის ან სხვა საგანგებო მდგომარეობაში უნივერსიტეტს დასაქმებულთა დაინფიცირების შესახებ ინფორმაციის შეგროვება შეუძლიათ დასაქმებულთა ნების მიუხედავად, თუ ეს ემსახურება უსაფრთხო შრომითი გარემოს უზრუნველყოფას ან/და ემსახურება ჯანმრთელობის დაცვის სისტემის მართვას.

უნივერსიტეტი უფლებამოსილია შეაგროვოს შემდეგი ინფორმაცია: დასაქმებული სტუმრობდა თუ არა ვირუსის გავრცელების მაღალ რისკის შემცველ ქვეყანას, აქვს თუ არა დასაქმებულს ვირუსის სიმპტომები, ჰქონდა თუ არა კონტაქტი ვირუსით დაინფიცირებულ პირ(ებ)თან. დასაქმებულის დაინფიცირების შესახებ ეჭვის შემთხვევაში უნივერსიტეტი მიმართავს შესაბამის ჯანდაცვის უწყებას და ექვემდებარება მათ მითითებებს.

მუხლი 6. შრომითი ურთიერთობებიდან გამომდინარე პერსონალური მონაცემები

1.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 ეფექტურად განხორციელებისა და სტუდენტთა ინტერესების დაცვითაა განპირობებული.

მუხლი 7. აბიტურიენტების/აპლიკანტების, სტუდენტებისა და კურსდამთავრებულების შესახებ პერსონალური მონაცემები

1.უნივერსიტეტის წესდებით გათვალისწიებული 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, არა სისტემატურად განსაკუთრებული კატეგორიის მონაცემებს, რაც სტუდენტის აკადემიური მიზნებითა და ინტერესებითაა განპირობებული.

მუხლი 8. მონაცემთა დამუშავების მიზნები

1.უნივერსიტეტის მიერ მონაცემები შესაძლოა დამუშავდეს შემდეგი მიზნ(ებ)ის მისაღწევად:

1.1. საგანმანათლებლო დაწესებულების სტატუსის მოპოვება (ავტორიზაცია), სასწავლებლის საქმიანობის შეუფერხებელი განხორციელება/ფუნქციონირება, საქართველოს კანონმდებლობით დაკისრებული მოვალეობების/ფუნქციების შესასრულებლად;

1.2. ვაკანტურ თანამდებობაზე თანამშრომლის შერჩევის პროცესის ორგანიზება, უნივერსიტეტში დასაქმებული პირების პირადი საქმეების მართვა, მოთხოვნად პოზიციებზე სარეზერვო ბაზების შექმნა და ორგანიზება, პერსონალის შეფასება, სახელშეკრულებო ურთიერობების ფარგლებში წამოჭრილი ნებისმიერი სხვა საკითხის გადასაწყვეტად (მივლინებები, შვებულებები, პერსონალის გამოკითხვა და სხვა);

1.3. საქმისწარმოების უზრუნველყოფა, დოკუმენტბრუნვის ორგანიზება და კონტროლი, უნივერსიტეტის საქმიანობის მარეგულირებელი აქტების შემუშავება, ფიზიკური და

იურიდიული პირების განცხადებების განხილვა, კონსულტაციების გაწევა სასწავლო პროცესებთან დაკავშირებულ საკითხებზე, უნივერსიტეტის წარმომადგენლობა სხვადასხვა ორგანოებთან და მესამე პირებთან ურთიერობაში;

1.4. შეფასებების წარმოება, პერონალის პროფესიული განვითარება, სტუდენტების მიღწევების შეფასება და ხარისხის კონტროლი, საბიბლიოთეკო საქმიანობის დაგეგმვა და მართვა;

1.5. სასწავლო გაზების მართვა, სასწავლებელში დასაქმებულ პირებთან და საგანმანათლებლო პროგრამების განხორციელებაში ჩართულ პირებთან ეფექტური კომუნიკაცია;

1.6. უნივერსიტეტის ტერიტორიაზე უსაფრთოების უზრუნველყოფა და პრევენცია, უნივერსიტეტის მხრიდან გაწერული მომსახურების ხარისხის გაუმჯობესება;

1.7.მარკეტინგული მიზნით, რაც გულისხმობს მონაცემთა სუბიექტის თანხმობით უნივერსიტეტის მიერ სხვადასხვა მარკეტინგული აქტივობების შემუშავებას/დაგეგმვას.

1.8. სხვა მიზნით, რაც განისაზღვრება შესაბამისი მონაცემთა დამუშავების დაწყებამდე.

2. უნივერსიტეტს უფლება აქვს დაამუშაოს მონაცემები პლაგიატის პრევენციისა და მისი გამოვლენის მიზნით.

3.უნივერსიტეტი უფლებამოსილია დაამუშაოს პერსონალური მონაცემები დისციპლინური ღონისძიებების გატარების დროს.

4.უნივერსიტეტი უფლებამოსილია კურსდამთავრებულებისათვის კარიერული ხელშეწყობის მიზნებისათვის ხელახლა დაამუშაოს პერსონალური მონაცემები. აწარმოოს კურსდამთავრებულთა დასაქმების მაჩვენებლების კვლევა.

5.უნივერსიტეტი ამუშავებს არასრულწლოვან პირთა მონაცემებს კანონიერი წარმომადგენლის თანხმობის საფუძველზე.

6.უნივერსიტეტი უზრუნველყოფს მუდმივად პერსონალური მონაცემთა დაცვის მონიტორინგის განხორციელებას.

მუხლი 9. მონაცემთა სუბიექტის უფლებები

1. მონაცემთა სუბიექტს ნებისმიერ დროს უფლება აქვს მიიღოს ინფორმაცია მის შესახებ დამუშავებული მონაცემების თაობაზე, კერძოდ:

1.1. რომელი მონაცემი მუშავდება და რა მიზნით;

1.2. მონაცემთა მოპოვების წყარო;

1.3. მონაცემთა შენახვის ვადა;

1.4. რა უფლებები გააჩნია მონაცემთა სუბიექტს დამუშავების მიმდინარეობისას;

1.5. ხდება თუ არა დამუშავება პროფილირების საფუძველზე;

1.6. ვის შეიძლება გადაეცეს (გადაეცემა) მისი მონაცემები და რა საფუძვლით;

1.7. გადაიცემა თუ არა მისი მონაცემები საერთაშორისო ორგანიზაციაში ან სხვა სახელმწიფოში და რა საფუძვლით.

2. ინფორმაციის მიღება დამატებით შესაძლებელია დამუშავების პროცესის, მისი ფორმებისა და მეთოდების შესახებ.

3. ინფორმაციის მიღების (მიწოდების) ფორმას (ელექტრონული, წერილობითი) ირჩევს მონაცემთა სუბიექტი.

4. მოთხოვილი ინფორმაცია სუბიექტს უნდა მიეწოდოს მოთხოვნისთანავე, გარდა იმ შემთხვევისა, როდესაც ინფორმაციის მიწოდება მოითხოვს მათ მოძიებას არქივში, სხვა სტრუქტურულ ერთეულში, ან საჭიროა დოკუმენტების კონსოლიდირება და დამუშავება. ამ შემთხვევაში ინფორმაციის მიწოდება უნდა განხორციელდეს არაუგვიანეს 10 სამუშაო დღის ვადაში.

5. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მის შესახებ არსებული მონაცემების გასწორება, განახლება, შევსება, დამატება, იმ შემთხვევაში თუ მონაცემები არაზუსტი ან არასრულია. თუ უნივერსიტეტი თავად ჩათვლის, რომ მონაცემები გასასწორებელი, განსაახლებელი, შესავსები ან დასამატებელია და თუ არსებობს საამისო მიზანი, 15 დღის ვადაში უნდა მოხდეს შესაბამისი ზომების მიღება მათი გასწორების, დამატების, შევსების ან/და განახლებისთვის.

6. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მონაცემთა დამუშავების დროებითი შეჩერება (დაბლოკვა) იმ შემთხვევაში, თუ სადავოა მონაცემთა დამუშავების მიზნები ან/და საფუძვლები, მათი ნამდვილობა ან სიზუსტე. უნივერსიტეტი, მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში, ახდენს მონაცემთა დაბლოკვას მოთხოვნიდან 3 დღის ვადაში.

7. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს მის შესახებ არსებული მონაცემების დამუშავების შეწყვეტა, წაშლა ან/და განადგურება.

8. მონაცემთა სუბიექტის უფლებების რეალიზაციისთვის მიმართვა უნდა განხორციელდეს უნივერსიტეტის მიმართ.

9. ამ მუხლით გათვალისწინებული სუბიექტის უფლებების შეზღუდვა დასაშვებია, თუ ამ უფლებების რეალიზებამ შეიძლება დააზიანოს ან/და საფრთხე შეუქმნას:

9.1. საზოგადოებრივი უსაფრთხოების ინტერესებს;

9.2. დანაშაულის თავიდან აცილებას, გამოძიებას, ოპერატიულ-სამძებრო საქმიანობას;

9.3. ქვეყნისთვის მნიშვნელოვან ფინანსურ და ეკონომიკურ ინტერესებს;

9.4. სახელმწიფო მარეგულირებელი ორგანოების, მათ შორის, განათლების სისტემის მარეგულირებელი ორგანოების უფლებამოსილებათა შესრულებას;

9.5. მონაცემთა სუბიექტის ან/და სხვათა უფლებებსა და თავისუფლებებს;

9.6. სახელმწიფო, კომერციული, პროფესიული და კანონით გათვალისწინებული სხვა სახის საიდუმლოების დაცვას;

9.7. მართლმსაჯულების განხორციელებას.

10. მონაცემთა სუბიექტს უფლება აქვს, კანონმდებლობით და ამ პოლიტიკით გათვალისწინებული უფლებებისა და განსაზღვრული წესების დარღვევის შემთხვევაში, საჩივრით მიმართოს უნივერსიტეტს.

11. მე-10 პუნქტით გათვალისწინებულ შემთხვევებში, საჩივრის წარდგენა შესაძლებელია, ასევე, სახელმწიფო ინსპექტორის სამსახურში ან/და სასამართლოში კანონმდებლობით დადგენილი წესით.

12. არასრულწლოვანი სტუდენტის შესახებ ინფორმაციის მიღების უფლება აქვს მშობელს, ან მის სხვა კანონიერ წარმომადგენელს. ხოლო სრულწლოვანი სტუდენტების შემთხვევაში, მათ შესახებ ინფორმაცია მშობლებს მიეწოდებათ, მხოლოდ სტუდენტის თანხმობით.

მუხლი 10. მონაცემთა შენახვა

1. პერსონალური მონაცემები ინახება როგორც ელექტრონული, ასევე მატერიალური ფორმით განსაზღვრული ვადით, უვადოდ და საარქივო მიზნებისათვის.

2. მონაცემთა შენახვის ვადები განისაზღვრება საქართველოს იუსტიციის მინისტრის 2010 წლის 31 მარტის #72 ბრძანებით.

3. მატერიალური სახით არსებული პერსონალური მონაცემები ინახება სპეციალურად გამოყოფილ კონტროლირებადი დაშვების დაცულ ადგილას.

მუხლი 11. დისტანციურად მუშაობისას მონაცემთა დამუშავება

1. დისტანციური მუშაობის განხორციელებისას უნივერსიტეტი, როგორც საგანმანათლებლო დაწესებულება უფლებამოსილია დისტანციური შეხვედრების გამართვისათვის გამოიყენოს სხვადასხვა ელექტრონული პლატფორმები (მაგალითად: Zoom, Teams, Moodle და აშ).

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 *(ამოქმედეს 2025წლის 1 მარტიდან).*

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 8 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.

7. საჭიროებისას უნივერსიტეტი უზრუნველყოფს უნივერსიტეტის უკაბელო ქსელური მოწყობილობის უსაფრთხოებას, კერძოდ:

ა). უკაბელო ქსელური მოწყობილობის სამართავ პანელზე წვდომა აქვს სამსახურის უფროსს ან მის მიერ გამოყოფილ პირს;

ბ). უკაბელო ქსელური კავშირისათვის გამოიყენება შიფრაციის თანამედროვე მეთოდები (მაგალითად, WPA2 ან WPA3);

გ). უკაბელო ქსელურ მოწყობილობასთან დაკავშირების პაროლი გამოიყენება კომპლექსური სახის, არანაკლებ 8 სიმბოლოსგან შემდგარი;

დ). პერიოდულად იცვლება უკაბელო ქსელის მოწყობილობასთან დაკავშირების პაროლი.

8. უნივერსიტეტში უკაბელო ქსელის დაცვისათვის, გატარებულია შემდეგი პოლიტიკა: ქსელი გაყოფილია 4 ნაწილად (ადმინისტრაცია, თანამშრომლები, სტუდენტები და საერთაშორისო ქსელი). შიდა ქსელში არსებულ ბაზებზე, მათ შორის სტუდენტთა მენეჯმენტის ბაზასთან წვდომა აქვს უნივერსიტეტის გარკვეულ პერსონალს, კონკრეტულ დონეზე. ამასთან ეს ბაზები დახურულია. ასევე პედაგოგებს, თავიანთ ჯგუფებზე, ხოლო სტუდენტებს მხოლოდ თავიანთ გვერდებზე.

9. უნივერსიტეტში ასევე დაცულია ელექტრონული დოკუმენტები. უნივერსიტეტში დოკუმენტბრუნვა წარმოებს ელექტრონული პროგრამა eflow-ს საშუალებით, პროგრამაში თითოეულ მომხმარებელს წვდომა აქვს, მხოლოდ მის ინდივიდუალურ პროფილთან, შესაბამისი პაროლის გამოყენებით.

მუხლი 12. მონაცემებზე წვდომის უფლების მქონე სუბიექტები

1. უნივერსიტეტის წინაშე მდგარი აკადემიური მიზნებისა და მისი ფუნქციონირების ეფექტიანობის უზრუნველსაყოფად, მონაცემებზე წვდომა საკუთარი კომპეტენციის ფარგლებში შესაძლებელია ჰქონდეს: რექტორს, ადმინისტრაციის ხელმძღვანელს (კანცლერს), ვიცე-რექტორებს, სასწავლო პროცესების მართვის, შეფასების და სტუდენტთა რეგისტრაციის დეპარტამენტს; ხარისხის უზრუნველყოფის სამსახურს; ადამიანური რესურსების მართვის სამსახურს; საინფორმაციო ტექნოლოგიების (IT) სამსახურს, ეკონომიკურ დეპარტამენტს; სტუდენტებთან და კურსდამთავრდებულებთან ურთიერობის სამსახურს; სამეცნიერო მუშაობის კოორდინაციის, მაგისტრატურისა და დოქტორანტურის სამსახურს; არქივს; იურიდიულ სამსახურს; სამეცნიერო განათლების კვლევისა და სტრატეგიული განვითარების დეპარტამენტს; საზოგადოებასთან ურთიერთობისა და პროტოკოლის სამსახურს; საერთაშორისო ურთიერთობების

დეპარტამენტს; უნივერსიტეტის ბიბლიოთეკას, უნივერსიტეტის ფაკულტეტებს: მედიცინის ფაკულტეტს, საზოგადოებრივი ჯანდაცვის ფაკულტეტს, სტომატოლოგიის ფაკულტეტს, ფარმაციის ფაკულტეტს, ფიზიკური მედიცინისა და რეაბილიტაციის ფაკულტეტს, სტომატოლოგიის საერთაშორისო ფაკულეტეტს, დიპლომირებული მედიკოსის ამერიკულ პროგრამას; მედიცინისა და სტომატოლოგიის საერთაშორისო ფაკულტეტს; დიპლომისშემდგომი სამედიცინო განათლებისა და უწყვეტი პროფესიული განვითარების ინსტიტუტს; აკადემიურ და მოწვეულ პროფესორ-მასწავლებლებს;

მუხლი 13. ვიდეოკონტროლისა და აუდიოკონტროლის განხორციელება.

1. სტუდენტებისა და სხვა პირთა უსაფრთხოების უზრუნველყოფის, საკუთრების დაცვის ან/და კონფიდენციალური ინფორმაციის დაცვის მიზნით, უნივერსიტეტის შენობის შიდა და გარე პერიმეტრზე, შემოსასვლელში და შენობის დერეფნებში წარმოებს ვიდეოკონტროლი.

2. აღნიშნული საკითხის მოწესრიგებულია, 2024 წლის 15 აგვისტოს სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის რექტორის #975693 ბრძანებით დამტკიცებული „სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტში ვიდეო/აუდიომონიტორინგის განხორციელების წესით“.

3. გამონაკლის შემთხვევებში, შესაბამისი წერილობითი დასაბუთებისა და საჭიროების გათვალისწინებით, აღნიშნული მუხლის პირველი პუნქტით გათვალისწინებული მიზნით, ვიდეოკონტროლის წარმოება დასაშვებია უშუალოდ სამუშაო ადგილას, თუ სხვაგვარად შეუძლებელია აღნიშნული მუხლის პირველ პუნქტში მითითებული მიზნების მიღწევა.

მუხლი 14. შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვა

1. უნივერსიტეტში დასაქმებული პირების სამუშაო ადგილზე დროული გამოცხადებისა და შესაბამის დროზე დატოვების, ასევე ნამუშევარი საათების გამოთვლის მიზნით შესაძლებელია წარმოებდეს ელექტრონული აღრიცხვა. აღრიცხვა შესაძლებელია განხორციელდეს ელექტრონული ბარათების გამოყენებით, რომელზეც დატანილი იქნება უნივერსიტეტში დასაქმებული პირის სახელი, გვარი, ბარათის უნიკალური ნომერი.

2. უნივერსიტეტი, კონტროლის განხორციელების მიზნით, აგროვებს შემდეგ მონაცემებს: სახელი, გვარი, ფოტოსურათი, საიდენტიფიკაციო დოკუმენტის ნომერი, სახე, შესვლისა და გასვლის თარიღები, დრო და მიზეზები.

3. უნივერსიტეტის შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვის მიზნით დაშვების სისტემაზე წვდომას ახორციელებს: დაცვის თანამშრომლები და ინფორმაციული ტექნოლოგიების სამსახური.

მუხლი 15. ელ-ფოსტისა და ტელეფონის ნომრის გამოყენება

1. ეფექტური და სწრაფი კომუნიკაციის მიზნით, უნივერსიტეტი ამუშავებს დასაქმებული პირების, აკადემიური, მოწვეული პერსონალის, თანაშემწეების, სტაჟიორების, მომსახურე პირების, სტუდენტებისა და კურსდამთავრებულების ელ - ფოსტებსა და ტელეფონის ნომრებს.

2. ელ-ფოსტისა და ტელეფონის ნომრის გამოყენება სიახლეების მიწოდებისა და სარეკლამო შეტყობინებების (პირდაპირი მარკეტინგი) გაგზავნის მიზნით დასაშვებია მხოლოდ სუბიექტის თანხმობით.

3. მონაცემთა სუბიექტს უფლება აქვს მოითხოვოს ელ-ფოსტის ან/და ტელეფონის ნომრის გამოყენების შეწყვეტა მარკეტინგული მიზნებისთვის, რაც დაუყონებლივ უნდა დაკმაყოფილდეს.

მუხლი 16. 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 შემთვევაში სისტემა უწყვეტად აგრძელებს მუშაობას მეორე მოწყობილობით. ნაკლებად კრიტიკული მოწყობილობის ჩანაცვლება კი ხდება საინფორმაციო ტექნოლოგიების სამსახურის მუდმივად განახლებადი, კონტროლირებადი მარაგიდან საკუთარი ძალით, დამოუკიდებლად. სისტემატურად ხორციელდება ძირითადი ქსელური აპარატურის კონფიგურაციის სარეზერვო ასლების შენახვა. დაზიანებული მოწყობილობების ახლით ჩანაცვლებისას აღნიშნული მონაცემების გამოყენება ამცირებს სერვისის წყვეტის დროს *(ამოქმედდეს 2025 წლის 1 მარტიდან)*.

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

3. ინფორმაციულ ტექნოლოგიებთან დაკავშირებული სავარაუდო რისკი შესაძლებელია იყოს ინფორმაციული სერვისების წყვეტა როგორც აპარატურული, ასევე პროგრამული უზრუნველყოფის დაზიანების და კიბერშეტევის გამო.

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 უსაფრთხოება; ვ) ქსელური აპარატურის კონფიგურაციების რეზერვირება; ზ) სერვერული აპარატურის სახანძრო მონიტორინგი; თ) სერვერული აპარატურის უწყვეტი ელ. მომარაგებით უზრუნველყოფა; ი) სერვერული სისტემების აპარატურული და პროგრამული განახლება; კ) ოპერაციული სისტემების განახლება; ლ) 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.

მუხლი 17. უსაფრთხოების ტექნიკური და ორგანიზაციული უზრუნველყოფა

1.უნივერსიტეტში უზრუნველყოფილია მონაცემთა დამუშავების ტექნიკური და ორგანიზაციული უსაფრთოების სტანდარტი, რომელიც მოქმედებს მონაცემთა დამუშავების მთელ ციკლზე.

2. უსაფრთხოების სტანდარტები ეფუძნება შემდეგ პრინციპებს:

2.1. მონაცემთა დაცვა, როგორც დამუშავების პროცესის განუყოფელი თვისება;

2.2.დამუშავების უსაფრთოებისათვის დანერგილი პროცედურების სრული ფუნქციონალურობა, დამუშავების მიზნებისათვის ან სუბიექტის უფლებების კომპრომისის გარეშე;

2.3. დამუშავების სრული ციკლის განმავლობაში ფუნქციონირება;

2.4. გამჭირვალობა და ანგარიშვალდებულება სუბიექტის წინაშე;

2.5.დამუშავების პროცესის ორიენტირება სუბიექტების უფლებათა დაცვის პრიორიტეტებიდან გამომდინარე;

3. უნივერსიტეტი უზრუნვლეყოფს ელექტრონული ფორმით არსებული მანაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვას, ხოლო არაელექტრონული ფორმით არსებულ მონაცემებთან მიმართულებით უზრუნველყოფს ყველა იმ მოქმედების აღრიცხვას, რომელიც უკავშირდება მათ გამჟღავნებას ან/და ცვლილებას.

4. უნივერსიტეტი, არაუმეტეს 6 თვიანი შუალედით, აფასებს მიღებული ტექნიკური და ორგანიზაციული უსაფრთხოების სტანდარტების ადეკვატურობასა და ეფექტიანობას, ხოლო საჭიროების შემთხვევაში, უზრუნველყოფს მათ განახლებას.

5. უსაფრთხოების ზომები მოიცავს შემდეგს:

5.1. პერსონალის ცნობიერების ამაღლებას ინფორმაციული უსაფრთხოების კუთხით. უნივერსიტეტში დასაქმებული პირების (მათ შორის აკადემიური და მოწვეული პერსონალის), უფლებამოსილი პირების, ასევე სტუდენტებისათვის ცნობიერების ასამაღლებელი შეხვედრებისა და შესაბამისი ტრენინგების ჩატარებას;

5.2. აკადემიური, მოწვეული თუ ადმინისტრაციული პერსონალისათვის მონაცემთა ელექტრონულ სისტემაში საკუთარ ანგარიშებზე შესასვლელად პაროლის სირთულის მინიმალური მოთხოვნების დაწესებას;

5.3. ლიცენზირებული პროგრამული უზრუნველყოფის გამოყენებას და უსაფრთხოების ზომების რეგულარულ განახლებას;

5.4. პერსონალური მონაცემების შემცველი დოკუმენტებისა და ფაილების უყურადღებოდ დატოვების აკრძალვას.

6. უნივერსიტეტში დასაქმებული ნებისმიერი პირი ვალდებულია აცნობიერებდეს მასზე დაკისრებულ პასუხისმგებლობას და არ დაუშვას პერსონალური მონაცემების დამუშავება, მათ შორის გამჟღავნება, კანონით გათვალისწინებული საფუძვლის არსებობის გარეშე.

მუხლი 18. პერსონალისა და სტუდენტების პასუხისმგებლობა

1. უნივერსიტეტში დასაქმებული პირები ვალდებულნი არიან დაიცვან უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკისა და სახელმძღვანელო პრინციპების დოკუმენტის მოთხოვნები, როგორც მათი ხელშეკრულების განუყოფელი ნაწილი.

2. 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.

3. პერსონალური მონაცემების დამუშავების შესახებ დადგენილი წესების დარღვევა არის უნივერსიტეტის პერსონალის მიმართ დისციპლინური დევნის დაწყების საფუძველი და შესაძლოა გახდეს შრომითი ურთიერთობების შეწყვეტის საფუძველი. უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკითა და სახელმძღვანელო პრინციპებით დადგენილი წესების დარღვევა არის სტუდენტის მიმართ დისციპლინური დევნის დაწყების საფუძველი.

მუხლი 19. პერსონალურ მონაცემთა დაცვის ოფიცერი

1.სუბიექტის უფლებების ეფექტური დაცვისა და პერონალურ მონაცემთა დაცვის კანონმდებლობის მოთხოვნათა ეფექტური შესრულების მიზნით, უნივერსიტეტში განსაზღვრულია პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი - პერსონალურ მონაცემთა დაცვის ოფიცერი, რომლის უფლება-მოვალეობები განსაზღვრულია „სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტში პერსონალურ მონაცემთა დაცვის წესით“ და პერსონალურ მონაცემთა დაცვის ოფიცრის შრომითი ხელშეკრულებით.

მუხლი 20. მონაცემთა საერთაშორისო გადაცემა

1. უნივერსიტეტის საქმიანობის მიზნებიდან გამომდინარე და შესაბამისი საფუძვლების გათვალისწინებით, დამუშავებული მონაცემები შესაძლებელია გადაიცეს საერთაშორისო ორგანიზაციისთვის ან/და სხვა სახელმწიფოში მყოფ/დაფუძნებულ პირთან, მათ შორის, კერძო ან საჯარო ორგანიზაციებთან.

2. უნივერსიტეტი უფლებამოსილია პერსონალური მონაცემები გადაუგზავნოს მხოლოდ იმ ქვეყნებს, რომელთა სიაც დამტკიცებულია, პერსონალური მონაცემთა დაცვის ინსპექტორის ბრძანებით N1 (16/09/2014წ.) - „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“.

3. მონაცემთა საერთაშორისო გადაცემისთვის უნივერსიტეტი იღებს შესაბამის ზომებს, რათა უზრუნველყოფილ იქნეს სუბიექტის უფლებების დაცვა და გადაცემის უსაფრთხოება.

4. მე-3 პუნქტით გათვალისწინებული მიზნით, უნივერსიტეტი საერთაშორისო გადაცემისთვის იღებს შემდეგ ზომებს:

4.1. აფასებს რისკებს, რომელიც დაკავშირებულია მონაცემთა საერთაშორისო გადაცემასთან;

4.2. აფორმებს შესაბამის ხელშეკრულებას მიმღებ მხარესთან, რომელიც, მათ შორის, ითვალისწინებს უნივერსიტეტისა და მიმღები მხარის უფლება-მოვალეობებს, სუბიექტის უფლებების დაცვის გარანტიებსა და გადაცემის შესაბამის მეთოდებს;

4.3. საჭიროების შემთხვევაში ათანხმებს და ნებართვას იღებს სახელმწიფო ინსპექტორისგან საერთაშორისო გადაცემის თაობაზე;

4.4. საჭიროების შემთხვევაში, აკონტროლებს გადაცემული პერსონალური მონაცემების დამუშავებას კანონმდებლობასთან თავსებადობის მიზნით, მათ შორის, გამოითხოვს ინფორმაციას დამუშავების პროცესთან დაკავშირებით.

5. უნივერსიტეტი აღრიცხავს მესამე პირებისათვის ინფორმაციის გაცემის ფაქტებს, თუ რა მონაცემი იქნა გაცემული, ვისთვის, როდის და რა სამართლებრივი საფუძვლით.

მუხლი 21. დასკვნითი დებულება

1. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტს, მის ცვლილებებს ამტკიცებს უნივერსიტეტის რექტორი.

2. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტში ცვლილებებისა და დამატებების შეტანა ხორციელდება საქართველოში მოქმედი კანონმდებლობით დადგენილი წესით, უნივერსიტეტის რექტორის ბრძანების საფუძველზე.

დანართი #1.

#	მონაცემთა სუბიექტი	პერსონალურ მონაცემთა დასახელება	შენახვის ვადები
1.	დასაქმებული	სახელი, გვარი	ხელმძღვანელობის

			მუდ. 74 წელი
2.	დასაქმებული	პირადი ნომერი	ხელმძღვანელობის მუდ. 74 წელი
3.	დასაქმებული	პირადობის მოწმობის ნომერი	ხელმძღვანელობის მუდ. 74 წელი
4.	დასაქმებული	მისამართი	ხელმძღვანელობის მუდ. 74 წელი
5.	დასაქმებული	ტელეფონის ნომერი	1 წელი ახლით შეცვლიდან
6.	დასაქმებული	პოზიცია	ხელმძღვანელობის მუდ.74 წელი
7.	დასაქმებული	ანაზღაურება	ხელმძღვანელობის მუდ. 74 წელი
8.	დასაქმებული	ელექტრონული ფოსტა	1 წელი ახლით შეცვლიდან
9.	დასაქმებული	პირადობის დამადასტურებელი დოკუმენტის ასლი	ხელმძღვანელობის მუდ. 74 წელი
10.	დასაქმებული	ფოტოსურათი	ხელმძღვანელობის მუდ. 74 წელი
11.	დასაქმებული	ავტობიოგრაფია	ხელმძღვანელობის მუდ. 74 წელი
12.	დასაქმებული	უმაღლესი განათლების, აკადემიური განათლების დამადასტურებელი დოკუმენტის ასლი	ხელმძღვანელობის მუდ. 74 წელი
13.	დასაქმებული	სამუშაო გამოცდილება	ხელმძღვანელობის მუდ. 74 წელი
14.	დასაქმებული	ინფორმაცია სემინარებსა და ტრენინგებში მონაწილეობის შესახებ	ხელმძღვანელობის მუდ. 74 წელი

15.	დასაქმებული	სამუშაო ადგილი	ხელმძღვანელობის მუდ. 74 წელი
16.	დასაქმებული	სამუშაო დრო	ხელმძღვანელობის მუდ. 74 წელი
17.	დასაქმებული	განათლების შესახებ ინფორმაცია	ხელმძღვანელობის მუდ. 74 წელი
18.	სამუშაოს მაძიებელი პირების მიერ მოწოდებული პერსონალური მონაცემები	ავტობიოგრაფია თანდართული დოკუმენტებით	ერთი წელი
19.	აკადემიური პერსონალი	დაკავებული თანამდებობა	ხელმძღვანელობის მუდ. 74.წელი
20.	აკადემიური პერსონალი	ინფორმაცია გავლილი სემინარებისა და ტრენინგების შესახებ	ხელშეკრულების შეწყვეტიდან ხელმძღვანელობის მუდ. 74 წელი
21.	სტუდენტი	სახელი, გვარი	უვადო
22.	სტუდენტი	პირადი ნომერი	უვადო
23.	სტუდენტი	ფოტოსურათი	სტატუსის შეწყვეტიდან 10 წელი
24.	სტუდენტი	დაბადების თარიღი	სტატუსის შეწყვეტიდან 10 წელი
25.	სტუდენტი	სქესი	სტატუსის შეწყვეტიდან 10 წელი
26.	სტუდენტი	ელექტრონული ფოსტის მისამართი	სტატუსის შეწყვეტიდან 10 წელი
27.	სტუდენტი	ტელეფონის ნომერი	სტატუსის შეწყვეტიდან 10 წელი

28.	სტუდენტი	მოქალაქეობა	სტატუსის შეწყვეტიდან 10 წელი
29.	სტუდენტი	მისამართი	სტატუსის შეწყვეტიდან 10 წელი
30.	სტუდენტი	სკოლის დამთავრების თარიღი	სტატუსის შეწყვეტიდან 10 წელი
31.	სტუდენტი	ატესტატის ნომერი	უვადო
32.	სტუდენტი	ატესტატის გაცემის თარიღი	სტატუსის შეწვეტიდან 10 წელი
33.	სტუდენტი	ჩარიცხვის ბრძანების თარიღი	უვადო
34.	სტუდენტი	ჩარიცხვის ბრძანების გაცემის თარიღო	უვადო
35.	სტუდენტი	სამხედრო აღრიცხვის ადგილი	სტატუსის შეწყვეტიდან 10 წელი
36.	სტუდენტი	უნივერსიტეტში ჩარიცხვის მეთოდი	უვადო
37.	სტუდენტი	სტატუსი	უვადო
38.	სტუდენტი	სწავლის საფასური	სტატუსის შეწყვეტიდან 10 წელი
39.	სტუდენტი	გრანტის შესახებ ინფორმაცია	სტატუსის შეწყვეტიდან 10 წელი
40.	სტუდენტი	ფაკულტეტი	უვადო
41.	სტუდენტი	სპეციალობა	უვადო

42.	სტუდენტი	ჯგუფი	სტატუსის შეწყვეტიდან 10 წელი
43.	სტუდენტი	პროგრამა	უვადო
44.	სტუდენტი	საფეხურის	უვადო
45.	სტუდენტი	სემესტრი	სტატუსის შეწყვეტიდან 10 წელი
46.	სტუდენტი	ბრძანების ნომერი სტუდენტის სტატუსის შეჩერების შესახებ	უვადო
47.	სტუდენტი	ბრძანების ნომერი სტუდენტის სტატუსის შეწყვეტის შესახებ	უვადო
48.	სტუდენტი	დიპლომი	უვადო
49.	სტუდენტი	დიპლომის დანართი	უვადო
50.	აკადემიური/ადმინი სტრაციული პერსონალი	აუდიოჩანაწერი	ერთი წელი
51.	სტუდენტი, თანამშრომელი, აკადემიური პერსონალი, ყოფილი თანამშრომელი, დებიტორი, კრედიტორის	სახელი, გვარი, საბანკო ანგარიშის ნომერი, ანაზღაურება	უვადო
52.	თანამშრომელი, სტუდენტი, ვიდეოთვალთვალის არეალში მოხვედრილი პირი	ვიდეოგამოსახულება	არაუმეტეს 20 დღე

53.	თანამშრომელი, სტუდენტი	შენობაში შესვლისა და შენობიდან გამოსვლის თარიღი და დრო	ერთი წელი
54.	თანამშრომელი, სტუდენტი	საიდენტიფიკაციო დოკუმენტის ნომერი	ერთი წელი
55.	თანამშრომელი, სტუდენტი	ჯანმრთელობის შესახებ მონაცემები	ერთი წელი
56.	დასაქმებული	შრომის დისციპლინის დოკუმენტები (აქტები, შეტყობინებები, ინფორმაციები, დახასიათებები, მოხსენებითი ბარათები, ცნობები, მიმოწერა	3 წელი
57.	დასაქმებული	პირადი საქმეები, განცხადებები, ავტობიოგრაფიები, ანკეტები, საატესტაციო ფურცლები	ხელმძღვანელი მუდ. 74 წელი
58.	დასაქმებული	დოკუმენტები, რომლებიც არ შევიდა პირადი საქმეების შემადგენლობაში (ცნობები, მოხსენებითი და განმარტებითი ბარათები, განცხადებები, სამივლინებო მოწმობები	5 წელი
59.	პირები	განცხადებები ვაკანტური თანამდებობის დასაკავებლად კონკურსში მონაწილების შესახებ	3 წელი
60.	დასაქმებული	შვებულების მიცემის	1 წელი

		გრაფიკი	
61.	დასაქმებული	სააღრიცხვო დოკუმენტები,ჟურნალები, ბარათები (პირების მიღების, გადაადგილების, დათხოვნის)	75 წელი
62.	დასაქმებული	სააღრიცხო დოკუმენტები, ჟურნალები, ბარათები (შვებულებები)	3 წელი
63.	დასაქმებული, სტუდენტი	დაშვების ბარათები (დაკარგვის შესახებ მოხსენებითი ბარათები, შეკვეთები)	1 წელი
64.	მხარეები	ხელშეკრულებები (მიწის, შენობის მფლობელობა, სარგებლობა)	უვადო
65.	მხარეები	ხელშეკრულებები, შეთანხმებები	ხელშეკრლების ვადის გავბლიდან 5 წელი
66.	ხელმძღვანელი	სხდომის ოქმი, დადგენილება, რეკომენდაცია, გადაწყვეტილება	უვადო
67.	ხელმძღვანელი	ბრძანება, მათთან დაკავშირებული დოკუმენტები	უვადო
68.	ხელმძღვანელი	ბრძანების პროექტები	3 წელი