ინფორმაციული უსაფრთხოების პოლიტიკა

ISO 9001 – ის მოთხოვნების მიხედვით

# 1. ვადები

# 1.1. დანიშნულება

1. ინფორმაციული უსაფრთხოების პოლიტიკა არის დოკუმენტი, რომელიც ხელმისაწვდომია უნივერსიტეტი-ს თანამშრომლებისთვის. ინფორმაციული უსაფრთხოების საკითხები, ინფორმაციული უსაფრთხოების მართვის სისტემის შექმნის პრინციპები, რომლებიც მიზნად ისახავს ორგანიზაციის ინფორმაციისა და სატელეკომუნიკაციო სისტემის უსაფრთხოების დაცვას, განაპირობებს სისტემების საიმედოობას და გამორიცხავს შეცდომების ტოლერანტობას; აგრეთვე იძლევა: ინფორმაციული აქტივების კონფიდენციალურობის, ინფორმაციის მთლიანობის, ხელმისაწვდომობის, ნამდვილობისა და მონიტორინგის უზრუნველყოფის საშუალებას.

2. პოლიტიკა განსაზღვრავს ძირითად პრინციპებს, რომელთა დაცვა უზრუნველყოფს ორგანიზაციის ინფორმაციული უსაფრთხოების საჭირო დონეს. ორგანიზაციის თანამშრომლების მიერ პოლიტიკის მოთხოვნების დაცვა, შექმნის პირობებს დაკისრებული დავალებების მაღალხარისხიანი შესრულებისათვის, უზრუნველყოფს მის სტაბილურობასა და მომგებიანობას.

# 1.2. მოქმედების სფერო

1. პოლიტიკა შემუშავებულია ISO / IEC 27001 სტანდარტის შესაბამისად, რომელიც ადგენს განვითარების, განხორციელების, გამოყენებისა და ოპტიმიზაციის ძირითად პრინციპებს, უნივერსიტეტის ინფორმაციის უსაფრთხოებას, ინფორმაციული ტექნოლოგიის დაცვის წესებს. ამ სტანდარტში მოცემული რეკომენდაციების შესაბამისად, პოლიტიკა განსაზღვრავს ინფორმაციის დაცვის ძირითად პრინციპებს (ნაწილებს). პოლიტიკის თითოეული ნაწილი განსაზღვრავს პროცესს, რომელიც უზრუნველყოფს IS სტანდარტით დადგენილ მოთხოვნებთან ყოველდღიური ოპერაციების შესაბამისობას, დონის შენარჩუნებას და წარმოადგენს უნივერსიტეტში IS– ს მიწოდების პროცესის ნაწილს.

2. უნივერსიტეტი ინახავს და ამუშავებს ინფორმაციას, რომელიც აუცილებელია ყოველდღიური საქმისწარმოებისთვის. ამ პოლიტიკის დებულებები ეხება მხოლოდ უნივერსიტეტის საქმიანობას კომერციული საიდუმლოების, პირადი მონაცემების, სხვა კონფიდენციალური ინფორმაციის შემცველი ინფორმაციის დაცვის სფეროში და არ მოქმედებს სახელმწიფო საიდუმლოების დაცვაზე.

3. ინფორმაციის დაცვა უნივერსიტეტის საქმიანობის სწორად წარმართვის აუცილებელი პირობაა. ინფორმაციული უსაფრთხოების დარღვევამ შეიძლება გამოიწვიოს სერიოზული ნეგატიური შედეგები, მათ შორის პირდაპირი მატერიალური ზიანი, დაინტერესებული მხარეების მხრიდან ნდობის დაკარგვა.

4. პოლიტიკა ითვალისწინებს უნივერსიტეტის ამჟამინდელ მდგომარეობასა და უახლოეს მომავალში საინფორმაციო ტექნოლოგიების განვითარებას, მიზნებს, ოპერაციულ პროცედურებს, მუშაობის რეჟიმებს და ასევე შეიცავს ინფორმაციას: უსაფრთხოების,

 საფრთხეების ანალიზის, ობიექტებისა და ინფორმაციული ურთიერთობების დეტალებზე.

5. დოკუმენტირებული IS ინფორმაცია უნდა შეესაბამებოდეს ამ პოლიტიკაში მითითებულ პრინციპებს.

# 1.3. ტერმინები, განმარტებები და აბრევიატურა

**ISMS** - ინფორმაციული უსაფრთხოების მართვის სისტემები

**IS** - ინფორმაციის უსაფრთხოება (კონფიდენციალურობის დაცვა, მთლიანობა და ინფორმაციის ხელმისაწვდომობა)

**IT -** საინფორმაციო ტექნოლოგია

**ITC** - ინფორმაციული და სატელეკომუნიკაციო სისტემები

**აქტივები** - რესურსი, რომელთა გამოყენებას მომავალში ეკონომიკური სარგებელი მოაქვს.

**მფლობელი** - ტერმინი განსაზღვრავს პირს ან სტრუქტურულ ერთეულს, რომელზეც ხელმძღვანელობის მიერ დამტკიცებულია პასუხისმგებლობა ამ რესურსის (აქტივის) განვითარების, შენარჩუნების, გამოყენებისა და უსაფრთხოების კონტროლისთვის.

# 1.4. მარეგულირებელი ცნობარი

**ISO / IEC 27001** საინფორმაციო ტექნოლოგია. ინფორმაციული უსაფრთხოების მართვის სისტემის დაცვის მეთოდები.

**ISO / IEC 27000** საინფორმაციო ტექნოლოგია. დაცვის მეთოდები. ინფორმაციული უსაფრთხოების მართვის სისტემები.

**2. პასუხისმგებლობისა და უფლებამოსილების დანაწილება**

1. უნივერსიტეტის ხელმძღვანელს ეკისრება პასუხისმგებლობა: კონტროლის, პოლიტიკის დებულებების მხარდაჭერის არსებულ მდგომარეობაში, კოორდინაციის და ინფორმაციული უსაფრთხოების მართვის პროცესებში - ცვლილებების შეტანის.

2. თანამშრომელთა პასუხისმგებლობა პოლიტიკაში მითითებული მოთხოვნებისა და რეკომენდაციების დარღვევის ან/და შეუსრულებლობისთვის გათვალისწინებულია შიდა ორგანიზაციული და ადმინისტრაციული დოკუმენტებით და სახელშეკრულებო ვალდებულებებით.

# 3. ინფორმაციული უსაფრთხოების ძირითადი მიზნები

1. ინფორმაციული უსაფრთხოების ძირითადი მიზნებია:

ა) უნივერსიტეტის ძირითადი ბიზნეს პროცესების უწყვეტობისა და უსაფრთხოების უზრუნველყოფა და იმ მოვლენების შესაძლო დანაკარგების შემცირება, რომლებიც საფრთხეს უქმნის უსაფრთხოებას.

ბ) ორგანიზაციის, მაღალი რეპუტაციის შენარჩუნება, რომელიც ორიენტირებულია საკუთარი ინფორმაციის, პარტნიორების, კონტრაქტორებისა და მომხმარებლების ინფორმაციის ეფექტურ დაცვაზე, რომელთანაც იგი მუშაობს.

2. ინფორმაციული უსაფრთხოების მთავარი მიზნის მისაღწევად, უნივერსიტეტის ამოცანებია:

ა) ინფორმაციის აქტივების კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობისა და ეფექტური გამოყენების უზრუნველყოფა;

ბ) ინფორმაციის კონფიდენციალურობის უზრუნველყოფა, კონფიდენციალური ინფორმაციის, მათ შორის პირადი მონაცემების გამჟღავნებით ზიანის თავიდან აცილება;

გ) უნივერსიტეტის მთლიანი ინფორმაციული ინფრასტრუქტურის მონიტორინგისა და დაცვის ეფექტური სისტემის შექმნა;

დ) უნივერსიტეტის პერსონალის ინფორმირებულობის დონის ამაღლება ინფორმაციული უსაფრთხოების საკითხებზე.

**4. ინფორმაციული უსაფრთხოების ფუნქციების და როლების განაწილება**

1. უნივერსიტეტის მენეჯმენტსა და თანამშრომლებს ესმით მათი ვალდებულებები, დაიცვან ინფორმაციული აქტივები და პირადად არიან პასუხისმგებლები ინფორმაციული უსაფრთხოების მოთხოვნების შეუსრულებლობაზე. ეს მოთხოვნები შედის შრომით ხელშეკრულებებში, აგრეთვე კონტრაქტორებთან ხელშეკრულებებში.

2. პოლიტიკის მოთხოვნები სავალდებულოა უნივერსიტეტის ყველა სტრუქტურული ერთეულისა და თანამშრომლებისთვის (სრული, დროებითი, კონტრაქტით მომუშავეები და ა.შ.), ასევე გარე მომხმარებლებისთვის (კონტრაქტორები, აუდიტორები და ა.შ.). ამ პოლიტიკით დადგენილი პროცედურა. პირთა ყველა ეს კატეგორია მონაწილეობს IS– ის უზრუნველყოფის პროცესში.

3. უნივერსიტეტის მენეჯმენტი აცნობიერებს ინფორმაციული აქტივების უსაფრთხოების უზრუნველყოფის მნიშვნელობას და ხელს უწყობს ISMS– ის მუდმივ გაუმჯობესებას.

# 4.1. პასუხისმგებელი ISMS– ის უზრუნველყოფის პროცესზე

ინფორმაციული ტექნოლოგიების დეპარტამენტი ახორციელებს, მხარს უჭერს და ზოგადად აკონტროლებს უნივერსიტეტის IT რესურსებში IS–ის უზრუნველყოფის პროცესს, აგრეთვე თანამშრომლებს აწვდის ინფორმაციას IS– ს საკითხებზე.

# 4.2. ფუნქციების განაწილება

1. უნივერსიტეტის ადმინისტრაცია:

ა) ამტკიცებს ინფორმაციული უსაფრთხოების პოლიტიკას, დებულებებს, პროცედურებს, ინსტრუქციებს და სხვა დოკუმენტურ ინფორმაციას;

ბ) ამტკიცებს რისკის მართვის სამოქმედო გეგმებს.

გ) პასუხისმგებელია ფინანსური და რესურსების მხარდაჭერაზე ინფორმაციული უსაფრთხოების რისკის მართვის სამოქმედო გეგმის განსახორციელებლად.

დ) დელეგირებს და განსაზღვრავს დაქვემდებარებულთა მოვალეობებს, უფლებებსა და პასუხისმგებლობებს ინფორმაციული უსაფრთხოების შესახებ.

2. ინფორმაციული ტექნოლოგიების დეპარტამენტი:

ა) შეიმუშავებს, კოორდინაციას და კონტროლს უწევს ინფორმაციული უსაფრთხოების პოლიტიკის, დებულების, პროცედურების, ინსტრუქციების განხორციელებას IS-ზე;

ბ) გადაწყვეტილებებს იღებს თითოეულ მნიშვნელოვან საფრთხეზე, ინფორმაციული უსაფრთხოების რისკის შეფასების ანგარიშებზე დაყრდნობით და ადგენს მენეჯმენტის შესაბამის სამოქმედო გეგმას;

გ) კოორდინაციას უწევს უნივერსიტეტის განყოფილებების მუშაობას ინფორმაციული უსაფრთხოების რისკის შეფასების მიმართულებით;

დ) განსაზღვრავს დანაყოფებში ინფორმაციული უსაფრთხოების მდგომარეობის შესაბამისობის დონეს ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნებთან და ანგარიშს აბარებს უფროს მენეჯმენტს;

ე) მოკვლევის შედეგების საფუძველზე, რეკომენდაციებს აძლევს ადმინისტრაციას ინფორმაციული უსაფრთხოების ინციდენტების გამოსწორების შესახებ.

3. უნივერსიტეტის თანამშრომლები:

ა) ვალდებულნი არიან, დაიცვან ინფორმაციული უსაფრთხოების პოლიტიკა და ორგანიზაციის სხვა პოლიტიკა;

ბ) ხელმძღვანელობენ IS-ის დებულებებით, პროცედურებით, ინსტრუქციებით სამუშაოების ყოველდღიურ შესრულებაში;

გ) საფრთხეების იდენტიფიცირება და მათი კვალიფიკაციის ფარგლებში ინფორმაციული უსაფრთხოების რისკების შეფასება;

დ) თანამშრომლები, რომლებმაც იციან ინფორმაციული უსაფრთხოების ინციდენტის შესახებ, ვალდებულნი არიან დაუყოვნებლივ მიიღონ ზომები ინციდენტის მიერ მიყენებული ზიანის შესამცირებლად, შეატყობინონ მომხდარი უნივერსიტეტის მენეჯმენტსა და ინფორმაციული ტექნოლოგიების დეპარტამენტს, თავიანთი კომპეტენციის ფარგლებში მოახდინონ რეაგირება ინფორმაციული აქტივების იდენტიფიცირებული და საეჭვო საფრთხეების შესახებ.

4. უნივერსიტეტის მენეჯმენტი აცნობიერებს, რომ ადამიანური ფაქტორი არის ერთ – ერთი ყველაზე გავლენიანი ფაქტორი ინფორმაციული უსაფრთხოების საფრთხეების განხორციელებაში და იღებს ზომებს ორგანიზაციული და ადმინისტრაციული დოკუმენტების მოთხოვნების შემუშავებისა და სისტემის პროგრამული უზრუნველყოფის, კომპიუტერული ტექნიკის გამოყენების წესის რეგულირების და ინფორმაციის დაცვისთვის; რეგულარულად აწვდის ინფორმაციას, აკონტროლებს და ამაღლებს თანამშრომელთა ინფორმირებულობას ინფორმაციული უსაფრთხოების შესახებ.

# 5. ინფორმაციული უსაფრთხოების პროცესის კომპონენტები

# 5.1. დაცვას დაქვემდებარებული ინფორმაციული ურთიერთობების ობიექტები

5.1.1. ინფორმაცია

ინფორმაციის დაცვის ერთიანი მოთხოვნების შემუშავების მიზნით, თანამშრომლების მიერ მათი ფუნქციური მოვალეობის შესრულების პროცესში შექმნილი, გამოყენებული, შენახული და განადგურებული მონაცემები უნდა განისაზღვროს (გადამამუშავებელი ცენტრისა და შესასვლელი ობიექტების მიერ) და კლასიფიცირდეს მათი ტიპისა და შეკვეთის მიხედვით. ამ მიზნით ორგანიზაცია შეიმუშავებს და აცნობებს ყველა პერსონალს "ინფორმაციის კლასიფიკაციის პროცედურის შესახებ", რომელიც ითვალისწინებს ისეთი კატეგორიის ინფორმაციის არსებობას, როგორიცაა: კონფიდენციალური ინფორმაცია (პირადი მონაცემების ჩათვლით, ტექნოლოგიური ინფორმაცია), საიდუმლოებები.

5.1.2. ორგანიზაციული და ტექნიკური წარმოების პროცესები

თითოეული თანამშრომლის, ისევე როგორც მთლიანად უნივერსიტეტის საქმიანობა ხასიათდება მრავალი განსაზღვრული ორგანიზაციული და ტექნიკური და წარმოების პროცესით. სტრუქტურული ერთეულების სტაბილური და უსაფრთხო მუშაობის უზრუნველსაყოფად ადეკვატური ზომების მისაღებად, ორგანიზაცია აფორმებს, აღწერს და აკონტროლებს (ინფორმაციული უსაფრთხოების თვალსაზრისით) ორგანიზაციულ და ტექნიკურ და საწარმოო პროცესებს.

5.1.3. ავტომატიზირებული სისტემები, პროგრამული უზრუნველყოფა და აპარატურა

პროგრამული უზრუნველყოფა და ტექნიკა (სერვერული და სატელეკომუნიკაციო მოწყობილობების ჩათვლით, უსაფრთხოების მოწყობილობა, საკომუნიკაციო არხები) ავტომატიზირებული (ინფორმაციული) სისტემები არსებული ორგანიზაციული, ტექნიკური და სასწავლო პროცესების შექმნის, შენარჩუნების, ავტომატიზაციისა და ოპტიმიზაციის ძირითადი საშუალებაა. დასაქმებულმა უნდა გააცნობიეროს საკითხის კრიტიკული ხასიათი და პროგრამული და აპარატურის განსაკუთრებული როლი უნივერსიტეტის ინფორმაციისა და სატელეკომუნიკაციო სისტემის ორგანიზებასა და ფუნქციონირებაში, მენეჯმენტი იღებს საჭირო ზომებს ამ უკანასკნელის დაკომპლექტების, სისწორისა და უსაფრთხოების კონტროლის მიზნით. ყველა პროგრამა და ტექნიკა აღირიცხება და იდენტიფიცირებულია. გარდა ამისა უნივერსიტეტის საქმიანობაში გამოყენებული ყველა ინფორმაცია, რომელიც კონკრეტულად არ იქნა დადგენილი, რომ საჯაროდ ხელმისაწვდომი ან სხვა იურიდიული და ფიზიკური პირების საკუთრებაა, არის უნივერსიტეტის საკუთრება.

# 5.2. ინფორმაციული ურთიერთობების საგნები

1. ორგანიზაციის ინფორმაციული უსაფრთხოების უზრუნველყოფისას ინფორმაციული ურთიერთობების სუბიექტებია:

ა) როგორც საინფორმაციო რესურსების მთავარი მფლობელი, ასევე მენეჯმენტი და უნივერსიტეტის თანამშრომლები;

ბ) იურიდიული და ფიზიკური პირები, რომლებიც მონაწილეობენ ორგანიზაციის ფუნქციონალური დავალებების შესრულებაში,

# 6. საფრთხის მოდელი

ორგანიზაცია თვლის საჭიროდ, რომ დაიცვას საკუთარი ინფორმაციული აქტივების, აგრეთვე მის პარტნიორებისა და მომხმარებლების მიერ მინდობილი ინფორმაციის ხელმისაწვდომობა, მთლიანობა, კონფიდენციალობა.

# 6.1. საფრთხეების ჩამონათვალი

1. კონფიდენციალურობის დარღვევა. საფრთხის შედეგი: არასანქცირებული (დამუშავება არ არის დაშვებული) მომხმარებლის მიერ ინფორმაციის ხელმისაწვდომობა და / ან მისი დამუშავების დადგენილი წესებისა და პროცედურების დარღვევა (გაჟონვა, გამჟღავნება).

2. მთლიანობის დარღვევა. საფრთხის შედეგი: ინფორმაციის შეცვლა და ინფორმაციის დაზიანება.

3. ინფორმაციის, პროცესის ან სისტემის ხელმისაწვდომობის დარღვევა. საფრთხის შედეგი: ინფორმაციის, სისტემის ან პროცესის წვდომის შეუძლებლობა და მათი სწორი გამოყენება.

# 6.2. საფრთხის წყაროები

*დამნაშავე* (არაკომპეტენტური თანამშრომელი; მოყვარული).

*შინაგანი თავდამსხმელი* (ინფორმაციული სისტემების ლეგიტიმური მომხმარებელი (ვისაც აქვს ანგარიში და წვდომის უფლება); თანამშრომელი, რომელსაც არ უშვებენ ინფორმაციულ სისტემებში, მაგრამ უფლება აქვს წვდომა ჰქონდეს უნივერსიტეტის ტერიტორიაზე და შენობაში (მათ შორის მომსახურე პერსონალი).

*გარე შემტევი* (ყოფილი თანამშრომლები; ორგანიზაციის წარმომადგენლები, რომელთანაც სამუშაო ხორციელდება სახელშეკრულებო და სხვა საფუძველზე) (კონტრაქტორები, პროვაიდერები); სტუმრები; კრიმინალური ჯგუფების წევრები, სხვა სახელმწიფოების სპეციალური სამსახურები ან მათი მითითებებით მოქმედი პირები;

კონკურენციის წარმომადგენელი ორგანიზაციები; პირები, რომლებმაც შემთხვევით ან განზრახ მოიპოვეს / სცადეს გარე ან მასთან დაკავშირებული სატელეკომუნიკაციო ქსელებიდან კორპორატიული ინფორმაციის სისტემებზე უნებართვო წვდომა).

# 6.3. საფრთხის ფაქტორები

უნებლიე (მცდარი, შემთხვევითი, უნებლიე) და / ან განზრახ (მესამე მხარის ან კანონით დაშვებული ინფორმაციული სისტემის მომხმარებელთათვის) ქმედებები, რომლებიც დაკავშირებულია ინფორმაციის უსაფრთხო დამუშავებისა და გადაცემის წესების დარღვევასთან, ინფორმაციული უსაფრთხოების წესების უგულებელყოფასთან, რამაც შეიძლება გამოიწვიოს კონფიდენციალურობის დარღვევა. ინფორმაციის მთლიანობა ან ხელმისაწვდომობა, აგრეთვე ორგანიზაციის ინფორმაციული და ტელეკომუნიკაციური სისტემის მუშაობის სტაბილური რეჟიმი.

განზრახ საფრთხის სახეები:

* + - ინფორმაციისა და სატელეკომუნიკაციო სისტემაში შეღწევა და მის ელემენტებსა და მასში მიმოქცეულ ინფორმაციაზე უნებართვო წვდომის მოპოვება;
		- დოკუმენტებისა და მედიის უნებართვო კოპირება; ინფორმაციის დამახინჯება; არასწორი მონაცემების შეყვანა;
		- კომპონენტების, აგრეთვე ქვესისტემების, რეგულარული მუშაობის დარღვევა მათი ფუნქციონირების უზრუნველსაყოფად (საინჟინრო სისტემები: ელექტროენერგიის მიწოდება, გაგრილება, ვენტილაცია, საკომუნიკაციო კაბელები და ა.შ.);
		- საკომუნიკაციო არხებით გადაცემული მონაცემების დაკვირვება და ანალიზი; ინფორმაციის უნებართვო მიღების ტექნიკური საშუალებების გამოყენება (ტექნიკური დაზვერვის საშუალებები);
		- სამრეწველო ნარჩენების ქურდობა (დოკუმენტების ბეჭდვა, სამუშაო ჩანაწერები, მედია);
		- წვდომის უფლებების დელიმიტაციის ატრიბუტების არასანქცირებული მიღება (აგენტის მიერ; მომხმარებელთა დაუდევრობის გამოყენება; შერჩევა ან გაყალბება);
		- ადამიანის სისუსტისა და უვიცობის გამოყენება ინფორმაციული უსაფრთხოების საკითხებში;
		- ლეგიტიმური მომხმარებლების ავტომატიზირებული სამუშაო ადგილებიდან ინფორმაციულ სისტემებსა და მის ელემენტებზე არასანქცირებული წვდომა;
		- კრიპტოგრაფიული საშუალებების (შიფრების) ქურდობა და / ან გატეხვა;
		- აპარატურისა და პროგრამული უზრუნველყოფის სანიშნეების დაყენება სისტემებსა და ინფორმაციაზე საიდუმლოდ წვდომის მიზნით;
		- ტექნიკის, ინფორმაციისა და საინჟინრო სისტემების და საკომუნიკაციო არხების უკმარისობა;
		- ხანძრები, წყალდიდობები, მიწისძვრები და სხვა სტიქიური მოვლენები.

# 7. ინფორმაციული უსაფრთხოების უზრუნველყოფა

1. ინფორმაციული უსაფრთხოების უზრუნველსაყოფად გამოიყენება პროცესუალური მიდგომა. ინფორმაციული სისტემების, ინფორმაციისა და პროცესების უსაფრთხოების მდგომარეობა მიიღწევა რიგი ორგანიზაციული და ტექნიკური ზომების სისტემატური გამოყენებით.

2. ამ ზომების რეგულირება მიიღწევა დოკუმენტაციის საშუალებით, პერსონალის სრული შემოწმების და ძირითადი პროცედურების რეგულარული კონტროლის მიზნით, ტექნიკური და წარმოების პროცესების, ავტომატიზირებული ინფორმაციული სისტემების, ინფორმაციის დამუშავების და ინფორმაციის აქტივების უწყვეტობის, სისწორისა და უსაფრთხოების უზრუნველსაყოფად.

# 7.1. ორგანიზაციული ღონისძიებები

7.1.1. მიმდინარეობა, ძირითადი საშუელებების ინფორმაციული დამუშავება. პასუხისმგებელი პირების დანიშვნა.

7.1.2. თანამშრომელთა ტრენინგი და პრაქტიკული კონტროლი: პროგრამული უზრუნველყოფისა, აპარატურისა, დაცვის საშუალებების, ინფორმაციის დამუშავებისა, ინფორმაციული უსაფრთხოების სწორად მუშაობის განხორციელებაში, ადამიანის სისუსტის გამოყენების ალბათობის შესამცირებლად. (თავდასხმები სოციალური ინჟინერიის მეთოდების გამოყენებით)

მოთხოვნები პერსონალის მიმართ: კორპორატიული ინფორმაციის, ტექნიკური დეტალების, ორგანიზაციის შესახებ ინფორმაციის, გუნდში მორალური და ფსიქოლოგიური კლიმატის დაუცველობის პრინციპის დაცვაზე.

7.1.3. უნივერსიტეტის ტერიტორიაზე და შენობაში შესვლის კონტროლისა და მართვის სისტემის დანერგვა; დეპოზიტის კონტროლი / მატერიალური ფასეულობების ამოღება.

7.1.4. პაროლის განახლებული პოლიტიკის შემუშავება და შენარჩუნება.

7.1.5. პერსონალის უსაფრთხოების უზრუნველყოფა (კანდიდატების შესწავლა, დაქირავება, გათავისუფლება).

# 7.2. ტექნიკური ზომები

7.2.1. ინფორმაციის ნაკადის ფიზიკური და / ან ლოგიკური გამიჯვნა, რაც დამოკიდებულია გადაცემული ინფორმაციის ტიპზე.

7.2.2. იდენტიფიკაცია, კონტროლი და დაცვა უნივერსიტეტის მისი სხვა მონაცემთა გადაცემის ქსელებთან დაკავშირების დროს; ზომების მიღება ITS– სთან არაავტორიზებული კავშირების თავიდან ასაცილებლად.

7.2.3. ტექნიკის, ინფორმაციული სისტემებისა და საკომუნიკაციო არხების ეფექტურობის მონიტორინგის უზრუნველყოფა; ინფორმაციის უსაფრთხოებასთან დაკავშირებული სისტემის მოვლენებისა და მოვლენების სისტემაში შესვლა (რეგისტრაცია) და რეგულარული ანალიზი.

7.2.4. ზომების მიღება ინფორმაციული უსაფრთხოების უზრუნველსაყოფად ინტერნეტ რესურსების, ელექტრონული ფოსტის და სხვა საშუალებების გამოყენებისას.

7.2.5. პროგრამული უზრუნველყოფის, აპარატურისა და ინფორმაციული სისტემების თანამშრომელთა წვდომის უფლებების დელიმიტაცია და კონტროლი ადმინისტრაციული პრივილეგიის მქონე პირთა ქმედებების კონტროლი. მომხმარებლებისთვის პრივილეგიების მინიჭება უნდა მოხდეს მაქსიმალური აუცილებლობის პრინციპზე.

7.2.6. ინფორმაციული უსაფრთხოების უზრუნველყოფა ელექტრონული გარიგების დროს. (პირველ რიგში, დისტანციური საბანკო სისტემებისთვის).

7.2.7. პროგრამებისა და ტექნოლოგიური სისუსტეების გამოყენებისგან დაცვას უზრუნველყოფს ანტივირუსული პროგრამები.

7.2.8. პროგრამული განახლების პროცედურის ორგანიზება და კონტროლი. ლიცენზირებული პროგრამული პროდუქტების გამოყენება. პროგრამული უზრუნველყოფისა და ტექნიკის უსაფრთხოების კონტროლი, ტექნიკური ხარვეზების ანალიზი და აღმოფხვრა.

7.2.9. უნივერსიტეტის ITS–ში ინფორმაციის შეყვანის / გამოტანის წესრიგის ორგანიზება და კონტროლი. ინფორმაციის გაცვლის პროცედურების აღწერა. ზომების მიღება ინფორმაციის გაჟონვის თავიდან ასაცილებლად მოსახსნელი საშუალებებით, ელექტრონული ფოსტით, მულტიმედიური კომუნიკაციის საშუალებით.

7.2.10. მოთხოვნების შემუშავება და ინფორმაციის სარეზერვო ასლის შეკვეთის რეგულირება და კონტროლი (მათ შორის, კონფიგურაციის ფაილები, სისტემის სურათები და ა.შ.). მიღებული ზომები რათა უზრუნველიყოს კონფიდენციალურობის, მთლიანობის, შესაბამისობისა და სარეზერვო ასლების არსებობა.

7.2.11. მომხმარებლების ტექნიკური დახმარების სისტემის დანერგვა. კომპიუტერული ინციდენტებზე რეაგირების პროცედურის შემუშავება და განხორციელება.

7.2.12. პროგრამული უზრუნველყოფისა და აპარატურის კონფიგურაციის აუცილებლობის გათვალისწინება, დეველოპერების მოთხოვნებისა და რეკომენდაციების შესაბამისად.

7.2.13. ორგანიზაციის ITS– ის უწყვეტი მუშაობის უზრუნველყოფა და ჩავარდნების შემდეგ რაც შეიძლება მალე მისი ეფექტურობის აღდგენა.