ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №1

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-4 მუხლის მე-2 პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების თანდართული მინიმალური მოთხოვნები.
2. ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №4 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **დავით ნადირაშვილი**

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

თავი I. ზოგადი დებულებები

მუხლი 1. მოქმედების სფერო

1. წინამდებარე ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები (შემდგომ – მოთხოვნები) ვრცელდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის (შემდგომ – კანონი) შესაბამისად იდენტიფიცირებულ, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტზე (შემდგომ – სუბიექტი).

2. მოთხოვნები ითვალისწინებს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტის (ISO 27000) განხორციელების საუკეთესო პრაქტიკას და მიზნად ისახავს სუბიექტის ინფორმაციული უსაფრთხოების დაცვის ქმედითი და ეფექტიანი განხორციელების მხარდაჭერას.

3. სუბიექტი ვალდებულია მოთხოვნები დანერგოს მისი „პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის დადგენილებით დამტკიცებულ ნუსხაში შეყვანის მომენტიდან 3 (სამი) კალენდარული წლის ვადაში, ამავე მოთხოვნებით გათვალისწინებული წესით.

მუხლი 2. ტერმინთა განმარტება

1. ამ მოთხოვნებსა და მის №1 დანართში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები – ინფორმაციული უსაფრთხოების მართვის სისტემის დასანერგად განსაზღვრული საბაზისო მოთხოვნები, რომლებიც სუბიექტმა უნდა

შეასრულოს თანმიმდევრულად;

ბ) ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომ – იუმს) – სუბიექტის შიდა (ორგანიზაციული) მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია რისკებისადმი სუბიექტის მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების მოთხოვნების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

გ) ინფორმაციული აქტივი (შემდგომ – აქტივი) – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სუბიექტისათვის;

დ) ხელმისაწვდომობა – უფლებამოსილი ერთეულის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი;

ე) კონფიდენციალურობა – მახასიათებელი, რომლის თანახმად ინფორმაცია სუბიექტის მიერ არ არის გამჟღავნებული ან ხელმისაწვდომი არაუფლებამოსილი ერთეულ(ებ)ისთვის;

ვ) მთლიანობა – ინფორმაციის, ინფორმაციული აქტივის სისწორისა და სისრულის მახასიათებელი;

ზ) ინფორმაციული უსაფრთხოება – ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შენარჩუნება და დაცვა, რაც დამატებით შესაძლოა მოიცავდეს ისეთ მახასიათებლებს, როგორებიცაა: ავთენტურობა, ანგარიშვალდებულება, წარმოშობის წყაროსთან ცალსახა შესაბამისობა და სანდოობა;

თ) რისკი – ამოცანის შესრულებასთან დაკავშირებული გაურკვევლობის ეფექტი;

ი) რისკის მფლობელი – რისკის მართვაზე ანგარიშვალდებული და უფლებამოსილი პირი ან მისი სტრუქტურული ერთეული;

კ) რეაგირების გარეშე ნარჩენი რისკი – რისკ(ებ)ის მოპყრობის შემდეგ დარჩენილი რისკი;

ლ) რისკის მიღება – სუბიექტის გაცნობიერებული გადაწყვეტილება გარკვეული რისკის მიღების თაობაზე;

მ) რისკის გამოვლენა – რისკის აღმოჩენის, გაცნობიერებისა და აღწერის პროცესი;

ნ) რისკის ანალიზი – რისკის არსის გაცნობიერებისა და რისკის დონის დადგენის პროცესი;

ო) რისკის დონის დადგენა – რისკის ანალიზის შედეგებისა და რისკის კრიტერიუმების შედარების პროცესი, რისკის ან/და მისი სიმძლავრის მისაღებობის ან მის მიმართ ტოლერანტობის დასადგენად;

პ) რისკის მართვა – სუბიექტის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკის გათვალისწინებით;

ჟ) რისკებთან მოპყრობა – რისკის ცვლილების პროცესი;

რ) კონტროლის მექანიზმი – ღონისძიება, რომელიც ცვლის რისკს;

ს) კონტროლის მექანიზმ(ებ)ის გამოყენებადობის განაცხადი – სუბიექტის იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი;

ტ) აუდიტი – ინფორმაციული უსაფრთხოების მართვის სისტემის შემოწმებისთვის მტკიცებულებების მოპოვებისა და მათი ობიექტურად შეფასების სისტემური, დამოუკიდებელი და დოკუმენტირებული პროცესი, რომელიც ადგენს, თუ რამდენად სრულდება შემოწმების კრიტერიუმები;

უ) შინასამსახურებრივი გამოყენების წესები – იუმს-ის ფარგლებში შემუშავებული დოკუმენტაცია (პოლიტიკა, პროცედურები, სახელმძღვანელოები და სხვა ინფორმაციის შემცველი მასალები),

რომელიც ემსახურება კანონის დებულებათა აღსრულებას;

ფ) დაინტერესებული მხარე – ნებისმიერი ფიზიკური ან იურიდიული პირი, ადმინისტრაციული ორგანო, რომელმაც შეიძლება გავლენა მოახდინოს სუბიექტის გადაწყვეტილებასა და ქმედებაზე; აგრეთვე, რომლის ინტერესზეც შესაძლოა გავლენა მოახდინოს სუბიექტის გადაწყვეტილებამ ან ქმედებამ;

ქ) სუბიექტის კრიტიკული ინფორმაციული სისტემა – ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია სუბიექტის ნორმალური ფუნქციონირებისათვის ან/და უზრუნველყოფს სუბიექტის ძირითადი საქმიანობის განხორციელებას.

2. ამ მოთხოვნებში გამოყენებულ სხვა ტერმინებს აქვს კანონით განსაზღვრული მნიშვნელობა.

თავი II. სუბიექტის მიერ პირველ წელს შესასრულებელი მოთხოვნები

მუხლი 3. მაღალი რგოლის მენეჯმენტის მხრიდან ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ორგანიზაციული მოწყობა

1. ამ მოთხოვნების გათვალისწინებით სუბიექტმა უნდა ჩამოაყალიბოს, დანერგოს, მხარი დაუჭიროს და მუდმივად გააუმჯობესოს ინფორმაციული უსაფრთხოების მართვის სისტემა.

2. იუმს-თან მიმართებით მაღალი რგოლის მენეჯმენტმა უნდა მოახდინოს ლიდერის როლისა და ნაკისრი ვალდებულების დემონსტრირება, რაც გამოიხატება შემდეგში:

ა) ინფორმაციული უსაფრთხოების პოლიტიკისა და ამოცანების ჩამოყალიბება და სუბიექტის სტრატეგიასთან შესაბამისობის უზრუნველყოფა;

ბ) იუმს-ის მოთხოვნების ინტეგრირება სუბიექტის მიერ განსახორციელებელ პროცესებში;

გ) იუმს-ისთვის საჭირო რესურსების ხელმისაწვდომობა;

დ) ეფექტიანი ინფორმაციული უსაფრთხოებისა და იუმს-ის მოთხოვნების მნიშვნელობის გაცნობიერება;

ე) იუმს-ის მიერ დასახული მიზნ(ებ)ის მიღწევა;

ვ) ჩართულ პირთა ხელმძღვანელობა და მხარდაჭერა, იუმს-ის ეფექტიანობის უზრუნველსაყოფად;

ზ) იუმს-ის მუდმივი გაუმჯობესების ხელშეწყობა;

თ) მენეჯმენტის სხვა წარმომადგენლების მხარდაჭერა, რათა უზრუნველყოფილ იქნეს მათი მხრიდან ლიდერობის გამომჟღავნება საკუთარი პასუხისმგებლობის ფარგლებში.

3. სუბიექტის მაღალი რგოლის მენეჯმენტმა უნდა განსაზღვროს პირი ან პირთა ჯგუფი (რომელიც დაკომპლექტებული იქნება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისაგან), რომელიც განახორციელებს იუმს-ის მხარდაჭერას.

4. მაღალი რგოლის მენეჯმენტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების შესაბამის პირებზე ან პირთა ჯგუფებზე პასუხისმგებლობებისა და უფლებამოსილებების განსაზღვრა და გაცნობა, რათა უზრუნველყოფილი იყოს იუმს-ის:

ა) შესაბამისობა ამ მოთხოვნებთან;

ბ) წარმადობის შესახებ ანგარიშგება მაღალი რგოლის მენეჯმენტთან.

მუხლი 4. იუმს-ის გავრცელების სფეროს განსაზღვრა

1. სუბიექტი ვალდებულია განსაზღვროს ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო და ამ პროცესში გაითვალისწინოს და გამოავლინოს:

ა) ორგანიზაციული კონტექსტი და გარემო ფაქტორები, რომლებიც მნიშვნელოვანია მისი მიზნებისთვის და გავლენას ახდენენ იუმს-ის მიერ დასახული შედეგების მიღწევაზე;

ბ) იუმს-ისთვის მნიშვნელოვანი დაინტერესებული მხარეები, მათი მოთხოვნები და მოლოდინები. დაინტერესებული მხარეების მოთხოვნები შესაძლოა მოიცავდეს როგორც საკანონმდებლო მოთხოვნებს, ასევე სახელშეკრულებო ხასიათის ვალდებულებებს;

გ) სუბიექტის საქმიანობა, ასევე სხვა ორგანიზაციასთან კავშირი და ურთიერთდამოკიდებულება.

2. იუმს-ის გავრცელების სფეროს დადგენისას, სუბიექტმა უნდა განსაზღვროს მასთან არსებული ყველა კრიტიკული ინფორმაციული სისტემა, ინფორმაციული აქტივი, პროცესი, ტექნოლოგია, პროდუქტი/სერვისი, მისი ორგანიზაციული სტრუქტურა და ადგილმდებარეობა, რომლებზეც ვრცელდება იუმს-ისთვის დადგენილი მოთხოვნები.

3. სუბიექტს იუმს-ის გავრცელების სფერო განსაზღვრული უნდა ჰქონდეს მატერიალური/ელექტრონული დოკუმენტის სახით, რომელსაც შეთანხმებისათვის წარუდგენს საჯარო სამართლის იურიდიულ პირს – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო).

მუხლი 5. ინფორმაციული უსაფრთხოების პოლიტიკა

1. სუბიექტის მაღალი რგოლის მენეჯმენტმა უნდა შეიმუშაოს და დაამტკიცოს ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც ეხმიანება სუბიექტის მიზანს და მოიცავს:

ა) ინფორმაციული უსაფრთხოების ამოცანებს ან აყალიბებდეს ინფორმაციული უსაფრთხოების ამოცანების განსაზღვრის ჩარჩოს;

ბ) ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მოთხოვნების შესრულებისთვის ნაკისრ ვალდებულებას;

გ) ინფორმაციული უსაფრთხოების მართვის სისტემის მუდმივი გაუმჯობესებისთვის ნაკისრ ვალდებულებას.

2. სუბიექტის მიერ დამტკიცებული ინფორმაციული უსაფრთხოების პოლიტიკა:

ა) უნდა არსებობდეს დოკუმენტირებული სახით;

ბ) უნდა იყოს ხელმისაწვდომი იუმს-ის გავრცელების სფეროში შემავალი ყველა პირისთვის;

გ) საჭიროების შემთხვევაში, ხელმისაწვდომი უნდა იყოს დაინტერესებული მხარისთვის.

3. ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისობის, ადეკვატურობისა და ეფექტიანობის უზრუნველყოფის მიზნით, მისი გადახედვა უნდა განხორციელდეს დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებებისას.

მუხლი 6. აქტივების მართვა

სუბიექტმა უნდა განახორციელოს იუმს-ის გავრცელების სფეროში გამოვლენილი აქტივების მართვა, რაც გულისხმობს აქტივების აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და დანერგვას, ამ მოთხოვნების №1 დანართის და „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად.

მუხლი 7. რისკების შეფასება

1. იუმს-ის დაგეგმვისას სუბიექტმა უნდა გაითვალისწინოს ორგანიზაციული კონტექსტი და გარემო ფაქტორები, დაინტერესებულ მხარეთა მოთხოვნები და მოლოდინები. ასევე, გამოავლინოს რისკები და ახალი შესაძლებლობები, რომლებზეც მოახდენს რეაგირებას, რათა:

ა) უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის საშუალებით დასახული შედეგების მიღწევა;

ბ) თავიდან აიცილოს ან შეამციროს არასასურველი გავლენა;

გ) უზრუნველყოს მუდმივი გაუმჯობესება;

დ) დაგეგმოს საპასუხო ქმედებები და განსაზღვროს მათი ინტეგრაციისა და დანერგვის საშუალებები, აგრეთვე შეაფასოს მათი ეფექტიანობა.

2. სუბიექტმა უნდა განსაზღვროს რისკების შეფასების პროცესი, რომელიც:

ა) აყალიბებს და ხელს უწყობს ინფორმაციული უსაფრთხოების რისკების მიღებისა და შეფასებისთვის საჭირო კრიტერიუმებს;

ბ) უზრუნველყოფს რისკების განმეორებითი შეფასებისას თანმიმდევრული, ვალიდური და შედარებადი შედეგების მიღებას;

გ) რისკის შეფასების პროცესის გამოყენებით გამოავლენს ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვასთან დაკავშირებულ ინფორმაციული უსაფრთხოების რისკებსა და რისკის მფლობელებს;

დ) აანალიზებს ინფორმაციული უსაფრთხოების რისკებს პოტენციური უარყოფითი შედეგებისა და რისკების ხდომილების ალბათობის ობიექტურად შეფასების გზით;

ე) ადგენს ინფორმაციული უსაფრთხოების რისკების დონეებს რისკების ანალიზის შედეგების შედარებით დადგენილ რისკების კრიტერიუმებთან, რომლის შედეგად გაანალიზებულ რისკებს ენიჭებათ პრიორიტეტები მათი შემდგომი მოპყრობისთვის.

3. სუბიექტმა ინფორმაციული უსაფრთხოების რისკების შეფასების პროცესი უნდა აღწეროს დოკუმენტირებული სახით.

მუხლი 8. რისკებთან მოპყრობა

1. სუბიექტმა უნდა განსაზღვროს და განახორციელოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის პროცესი, რათა:

ა) შეარჩიოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის სათანადო მეთოდები, რისკების შეფასების შედეგების გათვალისწინებით;

ბ) რისკების მოპყრობის შერჩეული მეთოდების დასანერგად გამოავლინოს, საკუთარი მოთხოვნების გათვალისწინებით, თავად შეიმუშაოს ან/და ნებისმიერი წყაროდან შეარჩიოს ყველა საჭირო კონტროლის მექანიზმი;

გ) გამოვლენილი კონტროლის მექანიზმები შეადაროს ამ მოთხოვნების №1 დანართით განსაზღვრულ კონტროლის მექანიზმებს და დარწმუნდეს, რომ ყველა მნიშვნელოვანი კონტროლის მექანიზმი გამოვლენილია. გარდა ამ მოთხოვნების №1 დანართში მითითებულისა, სუბიექტი უფლებამოსილია, თავად განსაზღვროს კონტროლის დამატებითი მიზნები და მექანიზმები;

დ) მოამზადოს კონტროლის მექანიზმების გამოყენებადობის განაცხადი, რომელშიც აღნიშნული იქნება ყველა აუცილებელი კონტროლის მექანიზმი, ასევე მათი შერჩევისა ან გამორიცხვის დასაბუთება

მიუხედავად მათი დანერგვის სტატუსისა;

ე) ჩამოაყალიბოს რისკების მოპყრობის გეგმა;

ვ) უზრუნველყოს რისკების მოპყრობის გეგმის დადასტურება და ნარჩენ რისკებზე თანხმობის მიღება რისკის მფლობელებისგან.

2. სუბიექტმა ინფორმაციული უსაფრთხოების რისკების მოპყრობის პროცესი უნდა აღწეროს დოკუმენტირებული სახით.

3. ამ მოთხოვნების მე-7 და მე-8 მუხლებში აღწერილი რისკების შეფასებისა და მოპყრობის პროცესი თავსებადობაშია ISO 31000-ში მოყვანილ პრინციპებსა და ზოგად სახელმძღვანელო მითითებებთან.

მუხლი 9. ინფორმაციული უსაფრთხოების ამოცანები და მათი შესრულების გეგმები

1. სუბიექტმა უნდა განსაზღვროს ინფორმაციული უსაფრთხოების ამოცანები შესაბამისი ფუნქციებისა და დონეებისთვის. ინფორმაციული უსაფრთხოების ამოცანები:

ა) შესაბამისობაში უნდა იყოს ინფორმაციული უსაფრთხოების პოლიტიკასთან;

ბ) უნდა იყოს გაზომვადი (თუ ეს შესაძლებელია);

გ) უნდა ითვალისწინებდეს ინფორმაციული უსაფრთხოების შესაბამის მოთხოვნებს, ასევე რისკების შეფასების და მათი მოპყრობის შედეგებს;

დ) უნდა არსებობდეს გაცხადებული სახით;

ე) უნდა იყოს განახლებული, საჭიროებისამებრ.

2. ინფორმაციული უსაფრთხოების ამოცანების მიღწევის გზების დაგეგმვისას სუბიექტმა უნდა განსაზღვროს:

ა) გასატარებელი ღონისძიებები;

ბ) საჭირო რესურსები;

გ) პასუხისმგებელი პირ(ებ)ი;

დ) ამოცანის მიღწევის ვადები;

ე) შედეგების შეფასების მეთოდი.

3. სუბიექტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების ამოცანების დოკუმენტირებული სახით არსებობა.

მუხლი 10. იუმს-ის მხარდაჭერა

1. სუბიექტმა უნდა განსაზღვროს და გამოყოს რესურსი იუმს-ის ჩამოყალიბების, დანერგვის, მხარდაჭერისა და მუდმივი გაუმჯობესებისთვის. ამ მიზნით, სუბიექტი ვალდებულია:

ა) განსაზღვროს იუმს-ში შემავალი პირების კომპეტენცია;

ბ) უზრუნველყოს პირების კვალიფიციურობა შესაბამისი ტრენინგებით, სწავლებითა და პრაქტიკული გამოცდილებით;

გ) საჭიროების შემთხვევაში, უზრუნველყოს პირების სათანადო კომპეტენცია (მათ შორის, ტრენინგის ჩატარების, იუმს-ის გავრცელების სფეროში შემავალი პირების სწავლების, ან სამსახურებრივი

პოზიციის ცვლილების, კომპეტენტური პირების დასაქმების ან ხელშეკრულების გაფორმების გზით) და შეაფასოს ამ მიზნით განხორციელებული ქმედებების ეფექტიანობა;

დ) შეინახოს იუმს-ის გავრცელების სფეროში შემავალ პირთა კომპეტენციის დამადასტურებელი დოკუმენტ(ები)ი.

2. იუმს-ის გავრცელების სფეროში შემავალ პირებს უნდა ჰქონდეთ ინფორმაცია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის შესახებ;

ბ) იუმს-ის ეფექტიანობის თვალსაზრისით საკუთარი ფუნქციების, მათ შორის, იუმს-ის მიზნების მიღწევაში შეტანილი წვლილისა და ინფორმაციული უსაფრთხოების წარმადობის შესახებ;

გ) იუმს-ის მოთხოვნების დარღვევით გამოწვეული უარყოფითი შედეგების შესახებ.

3. სუბიექტმა უნდა განსაზღვროს იუმს-ის ფარგლებში შიდა და გარე კომუნიკაციის საჭიროება, აგრეთვე:

ა) კომუნიკაციის საგანი;

ბ) კომუნიკაციის განხორციელების დრო;

გ) კომუნიკაციის წარმმართველი და ადრესატები;

დ) კომუნიკაციის წარსამართად საჭირო სხვა პროცესები.

მუხლი 11. სუბიექტის მიერ იუმს-ის დოკუმენტაციის მართვა

1. იუმს-ის ეფექტიანობის უზრუნველყოფის მიზნით, ის უნდა მოიცავდეს ამ მოთხოვნებით განსაზღვრულ, დოკუმენტირებულ და სუბიექტის მიერ დამატებით განსაზღვრულ სხვა ინფორმაციას.

2. ამ მუხლის პირველ პუნქტში მითითებული ინფორმაციის მოცულობას შესაძლოა განსაზღვრავდეს:

ა) სუბიექტის საქმიანობის ტიპი და მოცულობა, პროცესები, პროდუქტები და მომსახურებები;

ბ) პროცესების სირთულე და მათი ურთიერთქმედება;

გ) იუმს-ის გავრცელების სფეროში შემავალ პირთა კომპეტენცია.

3. დოკუმენტირებული ინფორმაციის შექმნისა და განახლებისას სუბიექტმა უნდა უზრუნველყოს დოკუმენტის:

ა) სათანადო ფორმით იდენტიფიკაცია და აღწერა (სათაური, თარიღი, ავტორი ან საიდენტიფიკაციო ნომერი);

ბ) შესაბამისი ფორმატი (ენა, პროგრამული უზრუნველყოფის ვერსია, გრაფიკული დიზაინი) და მედია-მატარებელი (მატერიალური ან/და ელექტრონული ფორმა);

გ) ადეკვატურობის განხილვა და დამტკიცება.

4. სუბიექტის მიერ იუმს-ის ფარგლებში განსაზღვრულ, დოკუმენტირებულ ინფორმაციაზე უნდა ხორციელდებოდეს კონტროლი, რათა:

ა) საჭიროების შემთხვევაში უზრუნველყოფილ იქნეს მისი ხელმისაწვდომობა და გამოყენებადობა;

ბ) სათანადოდ იყოს დაცული კონფიდენციალურობის დარღვევის, მთლიანობის დაკარგვისა და არასათანადოდ მოხმარებისგან.

5. დოკუმენტირებულ ინფორმაციაზე კონტროლის განხორციელების მიზნით, სუბიექტმა უნდა უზრუნველყოს:

ა) მისი სათანადო გავრცელება, წვდომა, გამოთხოვა და გამოყენება;

ბ) მისი შენახვის წესების დადგენა;

გ) დოკუმენტებში განხორციელებულ ცვლილებათა კონტროლი (ვერსიების კონტროლი);

დ) დოკუმენტების შენარჩუნება და განადგურება.

6. სუბიექტის მიერ უნდა ხორციელდებოდეს იუმს-ის დაგეგმვისა და ფუნქციონირებისთვის საჭიროდ მიჩნეული, გარე წყაროდან მიღებული, დოკუმენტირებული ინფორმაციის იდენტიფიცირება და მის გამოყენებაზე კონტროლი.

თავი III. სუბიექტის მიერ მეორე წელს შესასრულებელი მოთხოვნები

მუხლი 12. ინფორმაციულ უსაფრთხოებასთან დაკავშირებული პროცესების, გეგმების და ამოცანების აღსრულება

1. პირველ წელს შესასრულებელი მოთხოვნების დაკმაყოფილების შემდეგ, მეორე წელს სუბიექტი ვალდებულია:

ა) დაგეგმოს, დანერგოს და აკონტროლოს ინფორმაციული უსაფრთხოების მოთხოვნების დაკმაყოფილების პროცესი და გაატაროს ამ მოთხოვნების მე-7 და მე-8 მუხლებით განსაზღვრული ღონისძიებები;

ბ) განახორციელოს ამ მოთხოვნების მე-9 მუხლით განსაზღვრული გეგმები ინფორმაციული უსაფრთხოების ამოცანების შესასრულებლად;

გ) პროცესების გეგმის მიხედვით შესრულებასთან დაკავშირებით შეინახოს დოკუმენტირებული ინფორმაცია;

დ) აკონტროლოს დაგეგმილი ცვლილებები, განიხილოს გაუთვალისწინებელი ცვლილებებით გამოწვეული უარყოფითი შედეგები და საჭიროებისამებრ, მოახდინოს მათზე რეაგირება უარყოფითი გავლენის შესამცირებლად;

ე) გამოავლინოს მესამე მხარის მიერ განხორციელებული მომსახურება და უზრუნველყოს მათზე კონტროლი.

2. სუბიექტმა უნდა შეაფასოს ინფორმაციული უსაფრთხოების რისკები დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებების შემთხვევაში, ამ მოთხოვნების მე-7 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით დადგენილი კრიტერიუმების გათვალისწინებით. სუბიექტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების რისკის შეფასების შედეგების დოკუმენტირებული ფორმით არსებობა.

3. სუბიექტი ვალდებულია დანერგოს ინფორმაციული უსაფრთხოების რისკების მოპყრობის გეგმა და უზრუნველყოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის შედეგების დოკუმენტირებული ფორმით არსებობა.

მუხლი 13. სუბიექტის მიერ კონტროლის მექანიზმების დანერგვა

ინფორმაციული უსაფრთხოების მიზნების მისაღწევად სუბიექტი ვალდებულია:

ა) დანერგოს ამ მოთხოვნების მე-8 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტის შესაბამისად შერჩეული კონტროლის მექანიზმები;

ბ) კონტროლის მექანიზმების დანერგვისთანავე აწარმოოს მათზე დაკვირვება;

გ) გააანალიზოს დაკვირვების შედეგები და, საჭიროების შემთხვევაში, განსაზღვროს გაუმჯობესების გზები.

თავი IV. სუბიექტის მიერ მესამე წელს შესასრულებელი მოთხოვნები

მუხლი 14. ინფორმაციული უსაფრთხოების წარმადობისა და იუმს-ის ეფექტიანობის შეფასებისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა

1. ინფორმაციული უსაფრთხოების წარმადობისა და იუმს-ის ეფექტიანობის შეფასების მიზნით, სუბიექტმა უნდა განსაზღვროს:

ა) მონიტორინგის და შეფასების საგანი, მათ შორის, ინფორმაციული უსაფრთხოების პროცესები და კონტროლის მექანიზმები;

ბ) ვალიდური შედეგების მისაღწევად საჭირო მონიტორინგის, ანალიზისა და შეფასების ისეთი მეთოდები, რომლებიც უზრუნველყოფს შედარებადი და განმეორებადი შედეგის მიღწევას;

გ) მონიტორინგის და გაზომვის განხორციელების დრო;

დ) მონიტორინგისა და გაზომვის განმახორციელებელი პირ(ებ)ი;

ე) მონიტორინგის და გაზომვების შედეგების გაანალიზებისა და შეფასების დრო;

ვ) შედეგების გაანალიზებასა და შეფასებაზე პასუხისმგებელი პირ(ებ)ი.

2. სუბიექტმა უნდა უზრუნველყოს მონიტორინგისა და შეფასების შედეგების დოკუმენტირებული ფორმით არსებობა.

მუხლი 15. იუმს-ის შიდა აუდიტი

1. სუბიექტი ვალდებულია ჩაატაროს შიდა აუდიტი დაგეგმილი პერიოდულობით, ინფორმაციული უსაფრთხოების მართვის სისტემის თაობაზე შემდეგი ინფორმაციის მისაღებად:

ა) იუმს-ის სუბიექტის მიერ განსაზღვრულ მოთხოვნებთან შესაბამისობა;

ბ) იუმს-ის ამ მოთხოვნებთან შესაბამისობა;

გ) იუმს-ის ეფექტიანად დანერგვა და მისი მხარდაჭერა.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ვალდებულების გარდა, სუბიექტი აგრეთვე, ვალდებულია:

ა) დაგეგმოს, ჩამოაყალიბოს, დანერგოს და მართოს აუდიტის პროგრამა/პროგრამები, რაც გულისხმობს აუდიტის ჩატარების სიხშირის, მეთოდების, პასუხისმგებლობების, დაგეგმვის მოთხოვნების განსაზღვრასა და ანგარიშგებას. აუდიტის პროგრამაში/პროგრამებში გათვალისწინებული უნდა იყოს აუდიტის გავრცელების სფეროში შემავალი პროცესების მნიშვნელობა და წინა აუდიტის შედეგები;

ბ) დაადგინოს აუდიტის კრიტერიუმები და აუდიტის ფარგლები თითოეული აუდიტისთვის;

გ) შეარჩიოს აუდიტორები და ჩაატაროს აუდიტი ობიექტურად და მიუკერძოებლად;

დ) უზრუნველყოს აუდიტის შედეგების შესაბამისი ხელმძღვანელი პირების მიერ განხილვა;

ე) შეინახოს აუდიტის პროგრამ(ებ)ისა და აუდიტის შედეგების დოკუმენტირებული ინფორმაცია.

3. შიდა აუდიტი ტარდება სუბიექტის ან მესამე პირის მიერ სუბიექტის სახელით.

მუხლი 16. ხელმძღვანელობის მიერ იუმს-ის განხილვა

1. სუბიექტის მაღალი რგოლის მენეჯმენტმა დაგეგმილი პერიოდულობით უნდა განიხილოს იუმს-ი, რათა უზრუნველყოფილ იქნეს მისი მუდმივი შესაბამისობა, ადეკვატურობა და ეფექტიანობა. განხილვისას გათვალისწინებული უნდა იქნეს შემდეგი საკითხები:

ა) წინა განხილვის შემდგომ განხორციელებულ ღონისძიებათა სტატუსი;

ბ) ორგანიზაციული კონტექსტის და გარე ფაქტორების ცვლილებები, რომლებმაც შესაძლოა გავლენა იქონიონ ინფორმაციული უსაფრთხოების მართვის სისტემაზე;

გ) უკუკავშირი ინფორმაციული უსაფრთხოების წარმადობასთან დაკავშირებით, მათ შორის:

გ.ა) შეუსაბამობები და მაკორექტირებელი ქმედებები;

გ.ბ) მონიტორინგისა და გაზომვის შედეგები;

გ.გ) აუდიტის შედეგები;

გ.დ) ინფორმაციული უსაფრთხოების ამოცანების შესრულება.

დ) უკუკავშირი დაინტერესებული მხარეებისგან;

ე) რისკების შეფასების შედეგები და რისკებთან მოპყრობის გეგმის სტატუსი;

ვ) ახალი შესაძლებლობები გაუმჯობესებისთვის.

2. სუბიექტის მაღალი რგოლის მენეჯმენტის მხრიდან მუდმივი გაუმჯობესების შესაძლებლობებისა და მართვის სისტემის ცვლილებების საჭიროებების შესახებ განხილვის შედეგები უნდა აისახოს შესაბამისი გადაწყვეტილების ფორმით.

მუხლი 17. შეუსაბამობა და მაკორექტირებელი ქმედებები

1. აუდიტის შედეგად აღმოჩენილი შეუსაბამობის არსებობის შემთხვევაში სუბიექტი ვალდებულია:

ა) მოახდინოს მასზე რეაგირება, და შესაბამისად:

ა.ა) განახორციელოს ქმედებები შეუსაბამობის კორექტირებისთვის;

ა.ბ) გაუმკლავდეს და დაძლიოს შეუსაბამობით გამოწვეული უარყოფითი შედეგები;

ბ) შეაფასოს იმ ქმედებების საჭიროება, რომელთა მეშვეობითაც აღმოიფხვრება შეუსაბამობის მიზეზები მათი განმეორების თავიდან აცილების მიზნით. ამისათვის სუბიექტი ვალდებულია:

ბ.ა) განიხილოს შეუსაბამობა;

ბ.ბ) გამოავლინოს შეუსაბამობის მიზეზები;

ბ.გ) გამოავლინოს მსგავსი შეუსაბამობები ან მათი პოტენციური არსებობის შესაძლებლობა;

გ) შეფასების შედეგების საფუძველზე, შეუსაბამობების განმეორების თავიდან აცილების მიზნით, განახორციელოს საჭირო ქმედება;

დ) განიხილოს უკვე გატარებული მაკორექტირებელი ქმედებების ეფექტიანობა;

ე) საჭიროების შემთხვევაში განახორციელოს ცვლილებები ინფორმაციული უსაფრთხოების მართვის სისტემაში.

2. მაკორექტირებელი ქმედებები უნდა იყოს შეუსაბამობის გავლენის პროპორციული.

3. სუბიექტი ვალდებულია უზრუნველყოს დოკუმენტირებული ინფორმაციის არსებობა, რომლითაც დასტურდება:

ა) შეუსაბამობების ხასიათი და განხორციელებული ქმედებები;

ბ) გატარებული მაკორექტირებელი ქმედებების შედეგები.

მუხლი 18. მუდმივი გაუმჯობესება

სუბიექტმა მუდმივად უნდა გააუმჯობესოს ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისობა, ადეკვატურობა და ეფექტიანობა.

დანართი №1

კონტროლის მიზნები და მექანიზმები

1. შესავალი		
ინფორმაცია, მასთან დაკავშირებული პროცესები, სისტემები, ქსელები, ადამიანური რესურსი და სხვა ორგანიზაციული აქტივი სუბიექტისთვის წარმოადგენს ფასეულობას და საჭიროებს სათანადო დაცვას სუბიექტის წინაშე არსებული სხვადასხვა საფრთხისგან. ამასთან, ორგანიზაციული კონტექსტისა და გარე ფაქტორების ცვლილებებმა შესაძლოა წარმოშვან ახალი რისკები. ინფორმაციული უსაფრთხოების მართვის ეფექტიანი სისტემა ამცირებს ამგვარ რისკებს, იცავს სუბიექტს საფრთხეებისგან და მინიმუმამდე დაჰყავს არასასურველი გავლენა.		
2. მიზანი		
წინამდებარე დოკუმენტში ასახული კონტროლის მიზნები და მექანიზმები ხელს უწყობს იუმს-ის ეფექტიან მხარდაჭერას, რომელთა შერჩევისა და დანერგვისას სუბიექტმა უნდა გაითვალისწინოს მის წინაშე არსებული რისკები.		
3. კონტროლის მექანიზმების შერჩევა		
სუბიექტის მიზნების მისაღწევად საჭიროა კონტროლის მექანიზმების შერჩევა, ჩამოყალიბება, დანერგვა, მონიტორინგი, გადახედვა და საჭიროების შემთხვევაში, გაუმჯობესება, რაც, თავის მხრივ, უზრუნველყოფს ინფორმაციული უსაფრთხოების სათანადო დონის მიღწევას. სუბიექტმა კონტროლის მექანიზმების შერჩევისას უნდა იხელმძღვანელოს რისკის მართვის საუკეთესო პრაქტიკით, რისკის მიღების კრიტერიუმებით, რისკების მოპყრობის მეთოდებით და გაითვალისწინოს კანონმდებლობის მოთხოვნები. კონტროლის მექანიზმების შერჩევისას სუბიექტი უნდა დაეყრდნოს ამ დანართში მოცემულ კონტროლის მექანიზმებს, რათა არ მოხდეს მნიშვნელოვანი კონტროლის მექანიზმის გამოტოვება. ამასთან, ამ დანართში მოცემული კონტროლის მექანიზმების ჩამონათვალი შესაძლოა არ იყოს ამომწურავი და საჭირო გახდეს მათი შემუშავება ან შერჩევა სხვა წყაროდან.		
4. სტრუქტურა		
ამ დანართში მოცემული კონტროლის მიზნებისა და მექანიზმების ერთობლიობა მოიცავს უსაფრთხოების ძირითად კატეგორიებსა და კონტროლის მექანიზმებს. თითოეული პუნქტი შედგება უსაფრთხოების ერთი ან მეტი ძირითადი კატეგორიისგან, ხოლო თითოეული კატეგორია მოიცავს კონტროლის მიზანს და ერთ ან მეტ კონტროლის მექანიზმს. წარმოდგენილი კონტროლის მექანიზმების თანმიმდევრობა არ არის დალაგებული მათი მნიშვნელობისა და პრიორიტეტის გათვალისწინებით.		
5. ინფორმაციულ უსაფრთხოებასთან დაკავშირებული პოლიტიკის დოკუმენტები		
5.1 ხელმძღვანელობის ხედვა ინფორმაციულ უსაფრთხოებასთან დაკავშირებით		
მიზანი: ინფორმაციულ უსაფრთხოებასთან დაკავშირებით მაღალი რგოლის მენეჯმენტის ხედვის ჩამოყალიბება და მხარდაჭერა, საქმიანობასთან დაკავშირებული მოთხოვნების, ასევე საკანონმდებლო მოთხოვნების შესრულების უზრუნველსაყოფად.		
5.1.1	ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტი	*კონტროლის მექანიზმი* უნდა ჩამოყალიბდეს ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტების ერთობლიობა, დამტკიცდეს ხელმძღვანელობის მიერ, გამოქვეყნდეს და მიეწოდოს ყველა თანამშრომელს და ასევე, შესაბამის გარე დაინტერესებულ მხარეებს.
5.1.2	ინფორმაციული უსაფრთხოების	*კონტროლის მექანიზმი*

	პოლიტიკის დოკუმენტების გადახედვა	ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტების გადახედვა უნდა ხდებოდეს დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებებისას, რათა უზრუნველყოფილ იქნეს მისი შესაბამისობა, ადეკვატურობა და ეფექტიანობა.
6. ინფორმაციული უსაფრთხოების ორგანიზება		
6.1 შიდა ორგანიზება		
მიზანი: სუბიექტის მიერ ინფორმაციული უსაფრთხოების დანერგვისა და მისი შემდგომი ფუნქციონირების ჩამოყალიბებისა და კონტროლისთვის მართვის ჩარჩოს შექმნა.		
6.1.1	ინფორმაციული უსაფრთხოების როლები და პასუხისმგებლობები	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოების მიმართულებით არსებული ყველა პასუხისმგებლობა უნდა იყოს განსაზღვრული და განაწილებული შესაბამის პირ(ებ)ზე.
6.1.2	უფლება-მოვალეობების გამიჯვნა	*კონტროლის მექანიზმი* ურთიერთგამომრიცხავი მოვალეობები და პასუხისმგებლობები უნდა გაიმიჯნოს, რათა შემცირდეს სუბიექტის აქტივების არაავტორიზებული ან შემთხვევითი შეცვლის ან მათი ბოროტად გამოყენების შესაძლებლობა.
6.1.3	ურთიერთობა მნიშვნელოვან დაინტერესებულ მხარეებთან	*კონტროლის მექანიზმი* დაინტერესებულ მხარეებთან შესაბამისი კავშირების დამყარება და შენარჩუნება.
6.1.4	ურთიერთობა პროფესიულ ჯგუფებთან	*კონტროლის მექანიზმი* პროფესიულ ჯგუფებთან და უსაფრთხოების სპეციალისტთა ფორუმებთან, ასევე პროფესიულ ასოციაციებთან ურთიერთობის დამყარება და შენარჩუნება.
6.1.5	ინფორმაციული უსაფრთხოება პროექტების მართვაში	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოება გათვალისწინებულ უნდა იქნეს პროექტების მართვის პროცესში, პროექტის ტიპის მიუხედავად.
6.2 მობილური მოწყობილობები და დისტანციური მუშაობა		
მიზანი: დისტანციური მუშაობის და მობილური მოწყობილობების გამოყენების უსაფრთხოების უზრუნველყოფა.		
6.2.1	მობილური მოწყობილობების პოლიტიკა	*კონტროლის მექანიზმი* მობილური მოწყობილობების გამოყენებასთან დაკავშირებული რისკების მართვის მიზნით უნდა ჩამოყალიბდეს შესაბამისი პოლიტიკა და გატარდეს უსაფრთხოების ზომები.
6.2.2	დისტანციური მუშაობა	*კონტროლის მექანიზმი* დისტანციური მუშაობისას, ინფორმაციის დამუშავების, შენახვისა და მასზე წვდომისთვის, უნდა დაინერგოს შესაბამისი პოლიტიკა და გატარდეს უსაფრთხოების ზომები, ინფორმაციის დაცვის უზრუნველსაყოფად.
7. ადამიანური რესურსების უსაფრთხოება		
7.1 დასაქმებამდე		

მიზანი: თანამშრომლებისა და კონტრაქტორების მიერ პასუხისმგებლობების გაცნობიერებისა და ფუნქციებთან შესაბამისობის უზრუნველყოფა.		
7.1.1	გადამოწმება	*კონტროლის მექანიზმი* ყველა კანდიდატი უნდა მოწმდებოდეს კანონმდებლობისა და ეთიკის მოთხოვნათა დაცვით; შემოწმება პროპორციული უნდა იყოს კანდიდატის მიერ განსახორციელებელი საქმიანობის მოთხოვნების, წვდომადი ინფორმაციის კლასიფიკაციისა და წვდომასთან დაკავშირებული რისკებისა.
7.1.2	დასაქმების პირობები	*კონტროლის მექანიზმი* დასაქმებულებსა და კონტრაქტორებთან გაფორმებულ ხელშეკრულებებში მითითებული უნდა იყოს მხარეთა პასუხისმგებლობები ინფორმაციულ უსაფრთხოებასთან მიმართებით.
7.2 დასაქმების პერიოდში		
მიზანი: თანამშრომლებისა და კონტრაქტორების მიერ ინფორმაციულ უსაფრთხოებასთან დაკავშირებული პასუხისმგებლობების გაცნობიერება და შესრულება.		
7.2.1	ხელმძღვანელობის პასუხისმგებლობა	*კონტროლის მექანიზმი* ხელმძღვანელობამ უნდა მოსთხოვოს თანამშრომლებსა და კონტრაქტორებს ინფორმაციული უსაფრთხოების მოთხოვნების შესრულება სუბიექტის მიერ ჩამოყალიბებული უსაფრთხოების პოლიტიკებისა და პროცედურების შესაბამისად.
7.2.2	ცნობიერების ამაღლება, სწავლება და ტრენინგი ინფორმაციულ უსაფრთხოებაში	*კონტროლის მექანიზმი* სუბიექტის ყველა თანამშრომელი და საჭიროების შემთხვევაში, კონტრაქტორები ჩართულნი უნდა იყვნენ ცნობიერების ამაღლების პროგრამაში, მათთვის უნდა ტარდებოდეს ტრენინგი და იღებდნენ განათლებას შესაბამისი სწავლებით. ასევე, მათი ფუნქციების გათვალისწინებით, რეგულარულად უნდა მიეწოდოთ ინფორმაცია სუბიექტის პოლიტიკებისა და პროცედურების განახლებების შესახებ.
7.2.3	დისციპლინური პროცესი	*კონტროლის მექანიზმი* უნდა არსებობდეს ფორმალური და გაცხადებული დისციპლინური პროცესი და მიღებულ უნდა იქნეს ზომები იმ თანამშრომლების მიმართ, რომლებმაც დაარღვიეს ინფორმაციული უსაფრთხოება.
7.3 სამსახურიდან გათავისუფლება და დაკავებული თანამდებობის შეცვლა		
მიზანი: სუბიექტის ინტერესების დაცვა დაკავებული თანამდებობის შეცვლის ან სამსახურიდან გათავისუფლების პროცესში.		
7.3.1	დასაქმებულის თანამდებობიდან გათავისუფლება ან პასუხისმგებლობების ცვლილება	*კონტროლის მექანიზმი* უნდა განისაზღვროს ინფორმაციული უსაფრთხოების პასუხისმგებლობები და მოვალეობები, რომლებიც ძალაში რჩება შრომითი ურთიერთობის შეცვლის ან შეწყვეტის შემდეგ, მოხდეს მათ შესახებ თანამშრომლის ან კონტრაქტორის ინფორმირება და განხორციელდეს მათი აღსრულება.
8. აქტივების მართვა		

8.1 პასუხისმგებლობა აქტივებზე		
მიზანი: სუბიექტის აქტივების გამოვლენა და სათანადო დაცვაზე პასუხისმგებლობის განსაზღვრა.		
8.1.1	აქტივების გამოვლენა	*კონტროლის მექანიზმი* ინფორმაციასთან და ინფორმაციის დამუშავების საშუალებებთან დაკავშირებული აქტივები უნდა იყოს გამოვლენილი, შეიქმნას აქტივების რეესტრი და განხორციელდეს მისი მხარდაჭერა.
8.1.2	აქტივების მფლობელობა	*კონტროლის მექანიზმი* რეესტრში არსებულ აქტივებს უნდა ჰყავდეთ მფლობელები.
8.1.3	აქტივების სათანადო გამოყენება	*კონტროლის მექანიზმი* უნდა განისაზღვროს, დოკუმენტირებულად აღიწეროს და დაინერგოს ინფორმაციის და ინფორმაციის დამუშავებასთან დაკავშირებული აქტივების სათანადო გამოყენების წესები.
8.1.4	აქტივების დაბრუნება	*კონტროლის მექანიზმი* ყველა თანამშრომელმა და მესამე პირის წარმომადგენელმა შრომითი ურთიერთობის, ხელშეკრულების შეწყვეტის შემთხვევაში უნდა დააბრუნოს მათ განკარგულებაში არსებული სუბიექტის აქტივები.
8.2 ინფორმაციის კლასიფიკაცია		
მიზანი: ინფორმაციის მნიშვნელობიდან გამომდინარე სათანადო დაცვის დონის უზრუნველყოფა.		
8.2.1	ინფორმაციის კლასიფიკაცია	*კონტროლის მექანიზმი* ინფორმაციის კლასიფიკაცია უნდა მოხდეს საკანონმდებლო მოთხოვნების, მისი ფასეულობის, კრიტიკულობისა და სენსიტიურობის შესაბამისად, ასევე გათვალისწინებული უნდა იყოს უნებართვო გამჟღავნებისა ან ცვლილების შემთხვევები.
8.2.2	ინფორმაციის მარკირება	*კონტროლის მექანიზმი* სუბიექტის მიერ დადგენილი ინფორმაციის კლასიფიკაციის სქემასთან თავსებადი ინფორმაციის მარკირების სათანადო პროცედურები უნდა შემუშავდეს და დაინერგოს.
8.2.3	აქტივების მოპყრობა	*კონტროლის მექანიზმი* სუბიექტის მიერ დადგენილი ინფორმაციის კლასიფიკაციის სქემასთან თავსებადი აქტივების მოპყრობის პროცედურები უნდა შემუშავდეს და დაინერგოს.
8.3 მედია-მატარებლების მართვა.		
მიზანი: მედია-მატარებელზე არსებული ინფორმაციის უნებართვოდ გამჟღავნების, ცვლილების, წაშლის ან განადგურების თავიდან არიდება		
8.3.1	გადაადგილებადი მედია-მატარებლების მართვა	*კონტროლის მექანიზმი*

		სუბიექტის მიერ შემუშავებული კლასიფიკაციის სქემის შესაბამისად უნდა ჩამოყალიბდეს გადაადგილებადი მედია-მატარებლების მართვის პროცედურები.
8.3.2	მედია-მატარებლების განადგურება	*კონტროლის მექანიზმი* მედია-მატარებლების განადგურება უნდა მოხდეს უსაფრთხოდ, ფორმალიზებული პროცედურების გამოყენებით.
8.3.3	ფიზიკური მედია-მატარებლების გადაცემა	*კონტროლის მექანიზმი* ტრანსპორტირების დროს ინფორმაციის შემცველი მედია-მატარებელი დაცული უნდა იყოს უნებართვო წვდომისგან, არასათანადო გამოყენებისა ან დაზიანებისგან.
9. წვდომის კონტროლი		
9.1 წვდომის კონტროლისადმი განსაზღვრული საქმიანობის მოთხოვნები		
მიზანი: ინფორმაციასა და მისი დამუშავების საშუალებებზე წვდომის შეზღუდვა.		
9.1.1	წვდომის კონტროლის პოლიტიკა	*კონტროლის მექანიზმი* წვდომის კონტროლის პოლიტიკა უნდა ჩამოყალიბდეს დოკუმენტირებული სახით და უზრუნველყოფილ იქნეს მისი პერიოდული განხილვა საქმიანობისა და ინფორმაციული უსაფრთხოების მოთხოვნებიდან გამომდინარე.
9.1.2	წვდომა ქსელებზე და ქსელურ მომსახურებებზე	*კონტროლის მექანიზმი* მომხმარებლებს მხოლოდ იმ შემთხვევაში უნდა მიეცეთ წვდომა ქსელებსა და ქსელურ მომსახურებაზე, თუ მინიჭებული აქვთ შესაბამისი ნებართვა მათ გამოსაყენებლად.
9.2 მომხმარებელთა წვდომის მართვა		
მიზანი: სისტემებსა და მომსახურებებზე მომხმარებლების ნებადართული წვდომის უზრუნველყოფა და უნებართვო წვდომის თავიდან არიდება.		
9.2.1	მომხმარებლის რეგისტრაცია და მისი გაუქმება	*კონტროლის მექანიზმი* მომხმარებელთა რეგისტრაციისა და რეგისტრაციის გაუქმების ფორმალიზებული პროცესი უნდა დაინერგოს, რათა უზრუნველყოფილ იქნეს წვდომის უფლებების მინიჭება.
9.2.2	მომხმარებელთა წვდომის უზრუნველყოფა	*კონტროლის მექანიზმი* უნდა დაინერგოს სისტემასა და მომსახურებაზე მომხმარებლის წვდომის ფორმალიზებული პროცესი, რათა შესაძლებელი იყოს ყველა ტიპის მომხმარებლისთვის ყველა სისტემასა და მომსახურებაზე წვდომის უფლების მინიჭება ან გაუქმება.
9.2.3	პრივილეგირებული წვდომის უფლებების მართვა	*კონტროლის მექანიზმი* პრივილეგირებული წვდომის უფლებების მინიჭება და გამოყენება უნდა იყოს შეზღუდული და ექვემდებარებოდეს კონტროლს.
9.2.4	მომხმარებელთა საიდუმლო	*კონტროლის მექანიზმი*

	ავთენტიფიკაციის შესახებ ინფორმაციის მართვა	საიდუმლო ავთენტიფიკაციის შესახებ ინფორმაციის შეგროვება და განთავსება უნდა კონტროლდებოდეს მართვის ფორმალიზებული პროცესით.
9.2.5	მომხმარებლის წვდომის უფლებების გადახედვა	*კონტროლის მექანიზმი* აქტივების მფლობელები პერიოდულად უნდა ახდენდნენ მომხმარებელთა წვდომის უფლებების გადახედვას.
9.2.6	წვდომის უფლებების გაუქმება ან კორექტირება	*კონტროლის მექანიზმი* თანამშრომელთა და მესამე პირის წარმომადგენელთა წვდომის უფლებები ინფორმაციასა და ინფორმაციის დამუშავების საშუალებებზე უნდა გაუქმდეს შრომითი ან სახელშეკრულებო ურთიერთობის შეწყვეტისთანავე ან ცვლილების შესაბამისად, მოხდეს მათი კორექტირება.
9.3 მომხმარებელთა პასუხისმგებლობები		
მიზანი: მომხმარებლების მიმართ ანგარიშვალდებულების დაკისრება მათი ავთენტიფიკაციის შესახებ ინფორმაციის დაცვის უზრუნველსაყოფად.		
9.3.1	საიდუმლო ავთენტიფიკაციის ინფორმაციის გამოყენება	*კონტროლის მექანიზმი* მომხმარებლებს მოეთხოვებათ საიდუმლო ავთენტიფიკაციის შესახებ ინფორმაციის გამოყენება სუბიექტის მიერ დადგენილი წესების მიხედვით.
9.4 სისტემასა და პროგრამულ უზრუნველყოფაზე წვდომის კონტროლი		
მიზანი: სისტემასა და პროგრამულ უზრუნველყოფაზე უნებართვო წვდომის თავიდან არიდება.		
9.4.1	ინფორმაციაზე წვდომის შეზღუდვა	*კონტროლის მექანიზმი* ინფორმაციასა და პროგრამულ უზრუნველყოფაზე წვდომა უნდა იყოს შეზღუდული წვდომის კონტროლის პოლიტიკის შესაბამისად.
9.4.2	სისტემაში შესვლასთან დაკავშირებული უსაფრთხოების პროცედურები	*კონტროლის მექანიზმი* სისტემასა და პროგრამულ უზრუნველყოფაზე წვდომა უნდა კონტროლდებოდეს სისტემაში შესვლასთან დაკავშირებული უსაფრთხოების პროცედურებით, წვდომის კონტროლის პოლიტიკის შესაბამისად.
9.4.3	პაროლების მართვის სისტემა	*კონტროლის მექანიზმი* პაროლების მართვის სისტემა უნდა იყოს ინტერაქციული (დიალოგური) და უზრუნველყოფდეს პაროლების კომპლექსურობას.
9.4.4	პრივილეგირებული დამხმარე პროგრამების გამოყენება	*კონტროლის მექანიზმი* დამხმარე პროგრამების გამოყენება, რომლებსაც შეუძლიათ სისტემური ან პროგრამული კონტროლის მექანიზმების უგულებელყოფა, უნდა შეიზღუდოს და მკაცრად გაკონტროლდეს.
9.4.5	პროგრამულ კოდზე წვდომის კონტროლი	*კონტროლის მექანიზმი* პროგრამულ კოდზე წვდომა უნდა იყოს შეზღუდული.
10. კრიპტოგრაფია		

10.1 კრიპტოგრაფიული კონტროლის მექანიზმები		
მიზანი: ინფორმაციის კონფიდენციალურობის, ავთენტურობის ან/და მთლიანობის დაცვის უზრუნველსაყოფად კრიპტოგრაფიის სწორი და ეფექტიანი გამოყენება.		
10.1.1	კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენების პოლიტიკა	*კონტროლის მექანიზმი* ინფორმაციის დაცვის მიზნით უნდა შემუშავდეს და დაინერგოს კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენების პოლიტიკა.
10.1.2	გასაღებების მართვა	*კონტროლის მექანიზმი* უნდა შემუშავდეს და დაინერგოს კრიპტოგრაფიული გასაღების გამოყენების, დაცვისა და ექსპლუატაციის პერიოდის პოლიტიკა, რომელიც უნდა გატარდეს გასაღებების მთელ სასიცოცხლო ციკლზე.
11. ფიზიკური და გარემოს უსაფრთხოება		
11.1 დაცული არეები		
მიზანი: ინფორმაციასა და ინფორმაციის დამუშავების საშუალებებზე უნებართვო ფიზიკური წვდომის, დაზიანების ან ჩარევის თავიდან არიდება.		
11.1.1	ფიზიკური უსაფრთხოების პერიმეტრი	*კონტროლის მექანიზმი* უსაფრთხოების პერიმეტრი უნდა განისაზღვროს და გამოყენებულ იქნეს იმ არეების დასაცავად, სადაც განთავსებულია სენსიტიური ან კრიტიკული ინფორმაცია ან მისი დამუშავების საშუალებები.
11.1.2	ფიზიკური შესასვლელების კონტროლის მექანიზმები	*კონტროლის მექანიზმი* დაცული არეების უსაფრთხოება უზრუნველყოფილი უნდა იყოს შესასვლელების სათანადო კონტროლის მექანიზმებით, რათა მხოლოდ ავტორიზებულ პერსონალს ჰქონდეს წვდომის შესაძლებლობა.
11.1.3	ოფისების, ოთახების და მოწყობილობების დაცვა	*კონტროლის მექანიზმი* უნდა შემუშავდეს და გამოყენებულ იქნეს ოფისების, ოთახების და მოწყობილობების ფიზიკური დაცვის წესები.
11.1.4	გარე და ბუნებრივი საფრთხეებისგან დაცვა	*კონტროლის მექანიზმი* უნდა შემუშავდეს და გამოყენებული იქნეს სტიქიური უბედურებებისგან, მავნე პროგრამული შეტევისა ან უბედური შემთხვევისგან ფიზიკური დაცვის წესები.
11.l.5	დაცულ არეებში მუშაობა	*კონტროლის მექანიზმი* უნდა ჩამოყალიბდეს და გამოყენებულ იქნეს დაცულ არეებში მუშაობის პროცედურები.
11.1.6	ლოგისტიკური სივრცეები	*კონტროლის მექანიზმი* ლოგისტიკური და ასევე სხვა წვდომის სივრცეები, საიდანაც შესაძლოა განხორციელდეს პირთა უნებართვო შემოსვლა სუბიექტის ტერიტორიაზე, უნდა გაკონტროლდეს და, შეძლებისდაგვარად, მოხდეს ამ სივრცეთა

		იზოლირება ინფორმაციის დამუშავების საშუალებებისგან, რათა თავიდან იქნეს არიდებული უნებართვო წვდომა.
11.2 აპარატურა		
მიზანი: აქტივების დაკარგვის, ქურდობის ან საფრთხის ქვეშ დაყენების და სუბიექტის ოპერირების შეწყვეტის თავიდან არიდება.		
11.2.1	აპარატურის განთავსება და დაცვა	*კონტროლის მექანიზმი* აპარატურა განლაგებული და დაცული უნდა იყოს რისკებისგან, რომლებიც მომდინარეობს გარემოს საფრთხეებისგან, ასევე უნებართვო წვდომისგან.
11.2.2	დამხმარე მოწყობილობები	*კონტროლის მექანიზმი* დამუშავების საშუალებები დაცული უნდა იყოს ძაბვის ვარდნისა და სხვა გამანადგურებელი პროცესებისგან, რომელიც გამოწვეულია დამხმარე მოწყობილობებით.
11.2.3	კაბელების უსაფრთხოება	*კონტროლის მექანიზმი* ელექტროენერგიისა და მონაცემების გამტარი კაბელები დაცული უნდა იყოს მოპარვის, უნებართვო წვდომის ან დაზიანებისგან.
11.2.4	აპარატურის მხარდაჭერა	*კონტროლის მექანიზმი* აპარატურის განგრძობადი ხელმისაწვდომობისა და მთლიანობის უზრუნველსაყოფად უნდა განხორციელდეს მისი სწორი და სათანადო მხარდაჭერა.
11.2.5	აქტივების გადაადგილება	*კონტროლის მექანიზმი* წინასწარი ნებართვის გარეშე დაუშვებელია აპარატურის, ინფორმაციის ან პროგრამული უზრუნველყოფის გატანა სუბიექტის ტერიტორიის გარეთ.
11.2.6	სუბიექტის ტერიტორიის გარეთ არსებული აპარატურა და აქტივები	*კონტროლის მექანიზმი* სუბიექტის ტერიტორიის გარეთ არსებულ აქტივებზე, შესაბამისი რისკების გათვალისწინებით, უნდა ვრცელდებოდეს უსაფრთხოების წესები.
11.2.7	აპარატურის უსაფრთხო განადგურება ან ხელახლა გამოყენება	*კონტროლის მექანიზმი* განადგურებამდე ან ხელახლა გამოყენებამდე უნდა შემოწმდეს აპარატურაზე არსებული მედია საცავი, რათა უსაფრთხოდ გადაიწეროს ან წაიშალოს მასზე განთავსებული სენსიტიური ინფორმაცია და ლიცენზირებული პროგრამული უზრუნველყოფა.
11.2.8	უმეთვალყურეოდ დატოვებული აპარატურა	*კონტროლის მექანიზმი* მომხმარებლებმა უნდა უზრუნველყონ უმეთვალყურეოდ დატოვებული აპარატურის სათანადოდ დაცვა.
11.2.9	„სუფთა მაგიდისა“ და „სუფთა ეკრანის“ პოლიტიკა	*კონტროლის მექანიზმი*

		მიღებულ უნდა იქნეს ქაღალდზე არსებული მასალებისა და გადაადგილებადი მედია-მატარებლებისათვის „სუფთა მაგიდის პოლიტიკა“, ხოლო ინფორმაციის დამუშავების საშუალებებისათვის კი - „სუფთა ეკრანის პოლიტიკა“.
12. ოპერაციების უსაფრთხოება		
12.1 საოპერაციო პროცედურები და პასუხისმგებლობები		
მიზანი: ინფორმაციის დამუშავების მოწყობილობების გამართული და უსაფრთხო ფუნქციონირების უზრუნველყოფა.		
12.1.1	ოპერაციების ამსახველი დოკუმენტირებული პროცედურები	*კონტროლის მექანიზმი* ოპერაციების ამსახველი პროცედურები უნდა იყოს დოკუმენტირებული და ხელმისაწვდომი შესაბამისი საჭიროების მქონე მომხმარებლებისთვის.
12.1.2	ცვლილებების მართვა	*კონტროლის მექანიზმი* კონტროლს უნდა ექვემდებარებოდეს ორგანიზაციული და ბიზნეს პროცესების, ინფორმაციის დამუშავების საშუალებებსა და სისტემებში განხორციელებული/დაგეგმილი ის ცვლილებები, რომლებიც გავლენას ახდენენ ინფორმაციულ უსაფრთხოებაზე.
12.1.3	სიმძლავრეების მართვა	*კონტროლის მექანიზმი* რესურსების გამოყენება უნდა ექვემდებარებოდეს მონიტორინგს, გაუმჯობესებას, ასევე ხორციელდებოდეს მომავალი სიმძლავრეებისადმი მოთხოვნების პროგნოზირება, რათა უზრუნველყოფილ იქნეს სისტემის სათანადო წარმადობა.
12.1.4	პროგრამული უზრუნველყოფის შექმნის, ტესტირებისა და საოპერაციო გარემოთა გამიჯვნა	*კონტროლის მექანიზმი* პროგრამული უზრუნველყოფის შექმნის, ტესტირებისა და საოპერაციო გარემო უნდა იყოს გამიჯნული, რათა შემცირდეს საოპერაციო გარემოზე უნებართვო წვდომის ან მისი ცვლილების რისკები.
12.2 მავნე პროგრამული კოდისგან დაცვა		
მიზანი: ინფორმაციისა და ინფორმაციის დამუშავების საშუალებების დაცვა მავნე პროგრამული კოდისგან.		
12.2.1	მავნე პროგრამული კოდისგან დამცავი კონტროლის მექანიზმები	*კონტროლის მექანიზმი* მავნე პროგრამული კოდისგან დასაცავად საჭიროა დაინერგოს აღმომჩენი, პრევენციული და აღმდგენი კონტროლის მექანიზმები, რომელთა შესახებაც შესაბამისი მომხმარებლები უნდა იყვნენ ინფორმირებულნი.
12.3 სარეზერვო ასლი		
მიზანი: მონაცემების დაკარგვისგან დაცვა.		
12.3.1	ინფორმაციის სარეზერვო ასლი	*კონტროლის მექანიზმი* პერიოდულად უნდა ხორციელდებოდეს ინფორმაციის, პროგრამული უზრუნველყოფისა და სისტემის ანარეკლის („იმიჯები“) სარეზერვო ასლების აღება და მათი რეგულარული ტესტირება შეთანხმებული სარეზერვო ასლების წარმოების პოლიტიკის შესაბამისად.
12.4 ლოგირება და მონიტორინგი		

მიზანი: მოვლენების ჩაწერა და მტკიცებულებების წარმოება.		
12.4.1	მოვლენების ჩაწერა („ლოგირება“)	*კონტროლის მექანიზმი* მოვლენების ამსახველი ჩანაწერები („ლოგი“), რომელიც ასახავს მომხმარებელთა საქმიანობას, გამონაკლისებს, შეცდომებსა და ინფორმაციული უსაფრთხოების მოვლენებს, უნდა შეიქმნას, შეინახოს და რეგულარულად განიხილებოდეს.
12.4.2	ჩანაწერების („ლოგების“) ამსახველი ინფორმაციის დაცვა	*კონტროლის მექანიზმი* ჩანაწერები („ლოგები“) და მისი უზრუნველმყოფი მოწყობილობები დაცული უნდა იყოს ცვლილებისა და არაავტორიზებული წვდომისგან.
12.4.3	ადმინისტრატორისა და მომხმარებლის ჩანაწერები („ლოგები“)	*კონტროლის მექანიზმი* სისტემის ადმინისტრატორისა და მომხმარებლის საქმიანობათა შესახებ ჩანაწერები („ლოგები“) უნდა იწარმოებოდეს, დაცული იყოს და პერიოდულად ექვემდებარებოდეს განხილვას.
12.4.4	საათის სინქრონიზაცია	*კონტროლის მექანიზმი* სუბიექტის ან უსაფრთხო დომენის ფარგლებში არსებული ინფორმაციის დამუშავების სისტემების საათი სინქრონიზებული უნდა იყოს დროის ერთ სანდო წყაროსთან.
12.5 ოპერაციული სისტემების კონტროლი		
მიზანი: ოპერაციული სისტემების მთლიანობის უზრუნველყოფა.		
12.5.1	პროგრამული უზრუნველყოფის ინსტალაცია ოპერაციულ სისტემებში	*კონტროლის მექანიზმი* ოპერაციულ სისტემებზე პროგრამული უზრუნველყოფის ინსტალაცია უნდა კონტროლდებოდეს შესაბამისი პროცედურის გათვალისწინებით.
12.6 ტექნიკური სისუსტეების მართვა		
მიზანი: ტექნიკური სისუსტეების პრევენცია.		
12.6.1	ტექნიკური სისუსტეების მართვა	*კონტროლის მექანიზმი* დროულად უნდა იქნეს მოძიებული ინფორმაციული სისტემების ტექნიკური სისუსტეების შესახებ ინფორმაცია, აგრეთვე, უნდა შეფასდეს სუბიექტის დაუცველობა ამგვარი სისუსტეების მიმართ და გატარდეს სათანადო ღონისძიებები შესაბამის რისკებზე რეაგირებისთვის.
12.6.2	შეზღუდვები პროგრამული უზრუნველყოფის ინსტალაციაზე	*კონტროლის მექანიზმი* უნდა ჩამოყალიბდეს და დაინერგოს მომხმარებელთა მიერ პროგრამული უზრუნველყოფის ინსტალაციის განმსაზღვრელი წესები.
12.7 ინფორმაციული სისტემების აუდიტის მოთხოვნების გათვალისწინება		
მიზანი: ოპერაციულ სისტემებზე აუდიტის აქტივობების გავლენის შემცირება.		
12.7.1	ინფორმაციული სისტემების აუდიტის	*კონტროლის მექანიზმი*

	კონტროლის მექანიზმები	აუდიტის მოთხოვნები და აქტივობები, მათ შორის, ოპერაციული სისტემების შემოწმება, ყურადღებით უნდა დაიგეგმოს და შეთანხმდეს, რათა შემცირდეს ბიზნეს-პროცესის შეფერხების რისკი.
13. კომუნიკაციების უსაფრთხოება		
13.1 ქსელის უსაფრთხოების მართვა		
მიზანი: ქსელებში ინფორმაციის და ინფორმაციის დამუშავების საშუალებების დაცვა.		
13.1.1	ქსელის კონტროლი	*კონტროლის მექანიზმი* ქსელების მართვა უნდა კონტროლდებოდეს, რათა უზრუნველყოფილი იყოს ინფორმაციის დაცვა სისტემებსა და პროგრამულ უზრუნველყოფებში.
13.1.2	ქსელური მომსახურებების უსაფრთხოება	*კონტროლის მექანიზმი* ნებისმიერი ქსელური მომსახურების შესახებ შეთანხმებაში უნდა განისაზღვროს უსაფრთხოების მექანიზმები, მომსახურების დონეები და ხელმძღვანელობის მოთხოვნები, მიუხედავად იმისა, მომსახურების მომწოდებელი არის თავად სუბიექტი, თუ - მესამე პირი.
13.1.3	ქსელების გამიჯვნა	*კონტროლის მექანიზმი* ინფორმაციული მომსახურებების, მომხმარებლების და ინფორმაციული სისტემების ჯგუფები ქსელში უნდა იყოს გამიჯნული.
13.2 ინფორმაციის გადაცემა		
მიზანი: სუბიექტის შიგნით და მის გარეთ ინფორმაციის გადაცემის უსაფრთხოების უზრუნველყოფა.		
13.2.1	ინფორმაციის გადაცემის წესები და პროცედურები	*კონტროლის მექანიზმი* ინფორმაციის უსაფრთხო გადაცემა ნებისმიერი საკომუნიკაციო საშუალებით უზრუნველყოფილი უნდა იყოს ფორმალიზებული პოლიტიკით, პროცედურებითა და კონტროლის მექანიზმებით.
13.2.2	შეთანხმებები ინფორმაციის გადაცემის შესახებ	*კონტროლის მექანიზმი* საქმიანი ინფორმაციის უსაფრთხო გადაცემას უნდა არეგულირებდეს სუბიექტსა და მესამე პირებს შორის შეთანხმება.
13.2.3	ელექტრონული მიმოწერა	*კონტროლის მექანიზმი* ელექტრონულ შეტყობინებებში არსებული ინფორმაცია უნდა იყოს სათანადოდ დაცული.
13.2.4	შეთანხმებები ინფორმაციის კონფიდენციალურობის ან გაუმჟღავნებლობის შესახებ	*კონტროლის მექანიზმი* ინფორმაციის დაცვის კუთხით სუბიექტის საჭიროებაზე მორგებული, კონფიდენციალურობის ან გაუმჟღავნებლობის შესახებ სახელშეკრულებო მოთხოვნები უნდა იყოს შემუშავებული, რეგულარულად განხილული და დოკუმენტირებული.
14. ინფორმაციული სისტემების შეძენა, შექმნა და მხარდაჭერა		
14.1 ინფორმაციული სისტემების უსაფრთხოების მოთხოვნები		

მიზანი: ინფორმაციული უსაფრთხოების გათვალისწინება ინფორმაციული სისტემის მთელი სასიცოცხლო ციკლის მანძილზე. აღნიშნული ასევე მოიცავს მოთხოვნებს ინფორმაციული სისტემებისთვის, რომლებიც მომსახურებას გასწევენ საჯარო ქსელების მეშვეობით.		
14.1.1	ინფორმაციული უსაფრთხოების მოთხოვნების ანალიზი და მახასიათებლები	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოების მოთხოვნები გათვალისწინებული უნდა იყოს ახალი ინფორმაციული სისტემების ან არსებული სისტემების გაუმჯობესებისთვის.
l4.1.2	იმ პროგრამული უზრუნველყოფის დაცვა, რომელიც იყენებს საჯარო ქსელებს	*კონტროლის მექანიზმი* საჯარო ქსელების მეშვეობით გადაცემული ინფორმაცია უნდა იყოს დაცული თაღლითობისგან, ხელშეკრულების პირობების დარღვევის, არაავტორიზებული გამჟღავნებისა და ცვლილებისგან.
14.1.3	პროგრამული უზრუნველყოფის ტრანზაქციების დაცვა	*კონტროლის მექანიზმი* პროგრამული უზრუნველყოფის ტრანზაქციებში არსებული ინფორმაცია უნდა იყოს დაცული არასრული ინფორმაციის გადაგზავნისგან, არასწორი მარშრუტით გადაგზავნისგან, შეტყობინების არაავტორიზებული ცვლილებისა და გამჟღავნებისგან, დუბლირების ან არაავტორიზებული გამეორებისგან.
14.2 უსაფრთხოება პროგრამული უზრუნველყოფის შექმნასა და მხარდამჭერ პროცესებში		
მიზანი: ინფორმაციული სისტემების შექმნის პროცესში ინფორმაციული უსაფრთხოების ჩამოყალიბება და დანერგვა.		
14.2.1	უსაფრთხო „დეველოპმენტის“ პოლიტიკა (წესები)	*კონტროლის მექანიზმი* სუბიექტმა უნდა ჩამოაყალიბოს და გამოიყენოს პროგრამული უზრუნველყოფისა და სისტემების შემუშავების წესები.
14.2.2	სისტემის ცვლილების კონტროლის პროცედურები	*კონტროლის მექანიზმი* პროგრამული უზრუნველყოფის შექმნის პროცესში სისტემებში განხორციელებული ცვლილებები უნდა კონტროლდებოდეს ცვლილების კონტროლის ფორმალიზებული პროცედურის მიხედვით.
14.2.3	ოპერაციული პლატფორმის ცვლილებების შემდგომ პროგრამული უზრუნველყოფის ტექნიკური მიმოხილვა	*კონტროლის მექანიზმი* სუბიექტის ოპერაციებსა და უსაფრთხოებაზე უარყოფითი გავლენის თავიდან აცილების მიზნით, ოპერაციული პლატფორმის ცვლილებებისას, საქმიანობისთვის კრიტიკული პროგრამული უზრუნველყოფა, ერთი მხრივ, უნდა იყოს განხილული, ხოლო, მეორე მხრივ, უნდა განხორციელდეს მისი ტესტირება.
14.2.4	პროგრამული პაკეტების ცვლილებების შეზღუდვა	*კონტროლის მექანიზმი* პროგრამული პაკეტები უნდა შეიცვალოს და შეიზღუდოს მხოლოდ აუცილებლობის შემთხვევაში, ხოლო ყველა ცვლილება მკაცრად უნდა გაკონტროლდეს.

14.2.5	სისტემის უსაფრთხო შექმნის პრინციპები	*კონტროლის მექანიზმი* უსაფრთხო სისტემების შექმნის პრინციპები უნდა ჩამოყალიბდეს დოკუმენტირებული სახით, ასევე მხარდაჭერილი და გამოყენებული იყოს ნებისმიერი ინფორმაციული სისტემის დანერგვის პროცესში.
14.2.6	პროგრამული უზრუნველყოფის შექმნის უსაფრთხო გარემო	*კონტროლის მექანიზმი* სუბიექტმა უნდა ჩამოაყალიბოს და სათანადოდ დაიცვას პროგრამული უზრუნველყოფის შექმნის უსაფრთხო გარემო, სისტემის შემუშავებისა და ინტეგრაციისთვის, სისტემის შექმნის მთლიანი ციკლის გათვალისწინებით.
14.2.7	პროგრამული უზრუნველყოფის შექმნა მესამე მხარის მიერ („აუთსორსინგი“)	*კონტროლის მექანიზმი* სუბიექტმა უნდა განახორციელოს მონიტორინგი და ზედამხედველობა მესამე მხარის მიერ შექმნილ/შესაქმნელ პროგრამულ უზრუნველყოფაზე.
14.2.8	სისტემის უსაფრთხოების ტესტირება	*კონტროლის მექანიზმი* სისტემის უსაფრთხოების ტესტირება უნდა განხორციელდეს პროგრამული უზრუნველყოფის შექმნის პროცესში.
14.2.9	სისტემის ვარგისიანობის ტესტირება	*კონტროლის მექანიზმი* ახალი ინფორმაციული სისტემების, მათი განახლებებისა და ახალი ვერსიებისთვის უნდა ჩამოყალიბდეს სისტემის ვარგისიანობის პროგრამები და კრიტერიუმები.
14.3 სატესტო მონაცემები		
მიზანი: ტესტირებისთვის გამოყენებულ მონაცემთა დაცვის უზრუნველყოფა.		
14.3.1	სატესტო მონაცემების დაცვა	*კონტროლის მექანიზმი* სუბიექტმა სწორად უნდა შეარჩიოს სატესტო მონაცემები, უზრუნველყოს მათი დაცვა და კონტროლი.
15. მიმწოდებლებთან ურთიერთობები		
15.1 ინფორმაციული უსაფრთხოება მიმწოდებლებთან ურთიერთობისას		
მიზანი: მიმწოდებლისთვის ხელმისაწვდომი ორგანიზაციული აქტივების დაცვა.		
15.1.1	ინფორმაციული უსაფრთხოების პოლიტიკა მომწოდებლებთან ურთიერთობისას	*კონტროლის მექანიზმი* მომწოდებელთა მიერ სუბიექტის აქტივებზე წვდომისას წარმოშობილი რისკების შემცირების უზრუნველსაყოფად, სუბიექტმა დოკუმენტირებული სახით უნდა ჩამოაყალიბოს და მიმწოდებელთან შეათანხმოს ინფორმაციული უსაფრთხოების მოთხოვნები
15.1.2	მიმწოდებელთან ურთიერთობის ფარგლებში უსაფრთხოების	*კონტროლის მექანიზმი* სუბიექტმა უნდა ჩამოაყალიბოს ყველა შესაბამისი ინფორმაციული უსაფრთხოების მოთხოვნა და შეათანხმოს იმ მიმწოდებლებთან, რომლებსაც წვდომა აქვთ სუბიექტის ინფორმაციასთან, ასევე, ამუშავებენ, ინახავენ,

	მოთხოვნების გათვალისწინება	კომუნიკაციის პროცესში იყენებენ ამ ინფორმაციას ან ამ ინფორმაციის მისაწოდებლად ქმნიან IT ინფრასტრუქტურულ კომპონენტებს.
15.1.3	ინფორმაციული და საკომუნიკაციო ტექნოლოგიური საშუალებების მიწოდება	*კონტროლის მექანიზმი* მიმწოდებელთან დადებული ხელშეკრულებები უნდა მოიცავდეს ინფორმაციული უსაფრთხოების რისკებზე რეაგირების მოთხოვნებს, რომლებიც დაკავშირებულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების მომსახურებებსა და პროდუქტის მოწოდებასთან.
15.2 მიმწოდებლის მომსახურების მართვა		
მიზანი: უზრუნველყოფილი იქნეს ინფორმაციული უსაფრთხოების დონის შენარჩუნება და მომსახურების მიწოდების შეთანხმებული დონის მხარდაჭერა მომსახურების ხელშეკრულების შესაბამისად.		
15.2.1	მიწოდებული მომსახურების მონიტორინგი და მიმოხილვა	*კონტროლის მექანიზმი* სუბიექტმა რეგულარულად უნდა განახორციელოს მიწოდებული მომსახურების მონიტორინგი, მიმოხილვა და აუდიტი.
15.2.2	მიწოდებასთან დაკავშირებული მომსახურების ცვლილებების მართვა	*კონტროლის მექანიზმი* მიმწოდებლის მიერ მომსახურებებში ცვლილებების შეტანისას, მათ შორის არსებული ინფორმაციული უსაფრთხოების პოლიტიკის, პროცედურების და კონტროლის მექანიზმების მხარდაჭერისა და გაუმჯობესებისას გათვალისწინებული უნდა იყოს ინფორმაციის, სისტემებისა და პროცესების კრიტიკულობა რისკების ხელახალი შეფასების გზით.
16. ინფორმაციული უსაფრთხოების ინციდენტების მართვა		
16.1 ინფორმაციული უსაფრთხოების ინციდენტების მართვა და გაუმჯობესება		
მიზანი: თანმიმდევრული და ეფექტიანი მიდგომით, ინფორმაციული უსაფრთხოების ინციდენტების მართვა, მათ შორის უსაფრთხოების მოვლენების და სისუსტეების შესახებ კომუნიკაციის უზრუნველყოფა.		
16.1.1	პასუხისმგებლობები და პროცედურები	*კონტროლის მექანიზმი* უნდა ჩამოყალიბდეს ხელმძღვანელობის პასუხისმგებლობები და პროცედურები, რათა მოხდეს სწრაფი, ეფექტიანი და სათანადო რეაგირება ინფორმაციული უსაფრთხოების ინციდენტზე.
16.1.2	ინფორმაციული უსაფრთხოების მოვლენების შესახებ ანგარიშგება	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოების მოვლენების შესახებ ანგარიშგება უნდა განხორციელდეს დროულად შესაბამისი საკომუნიკაციო არხების მეშვეობით.
16.1.3	ინფორმაციული უსაფრთხოების სისუსტეების შესახებ ანგარიშგება	*კონტროლის მექანიზმი* სუბიექტის ინფორმაციული სისტემის და მომსახურების მომხმარებლები, მათ შორის, თანამშრომლები და კონტრაქტორები, ვალდებულნი არიან აცნობონ სუბიექტს აღმოჩენილი ან სავარაუდო უსაფრთხოების სისუსტის შესახებ.
16.1.4	ინფორმაციული უსაფრთხოების მოვლენების შეფასება	*კონტროლის მექანიზმი*

	და გადაწყვეტილების მიღება	სუბიექტმა უნდა შეაფასოს ინფორმაციული უსაფრთხოების მოვლენები და მიიღოს გადაწყვეტილება მათი ინფორმაციული უსაფრთხოების ინციდენტად კლასიფიცირებაზე.
16.1.5	ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირება	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირება უნდა მოხდეს დოკუმენტირებული პროცედურების შესაბამისად.
16.1.6	ინფორმაციული უსაფრთხოების ინციდენტებიდან ცოდნის და გამოცდილების მიღება	*კონტროლის მექანიზმი* ინფორმაციული უსაფრთხოების ინციდენტების აღმოფხვრის და ანალიზის შედეგად მიღებული ცოდნა გამოყენებული უნდა იყოს მომავალი ინციდენტების ალბათობის და გავლენის შესამცირებლად.
16.1.7	მტკიცებულებათა შეგროვება	*კონტროლის მექანიზმი* სუბიექტმა უნდა განსაზღვროს და გამოიყენოს ინფორმაციის გამოვლენის, შეგროვების, მოძიების და შენახვის პროცედურები, რომელიც, თავის მხრივ, შესაძლოა გამოყენებულ იქნეს მტკიცებულებად.
17. ინფორმაციული უსაფრთხოების ასპექტები საქმიანობის უწყვეტობის მართვაში		
17.1 ინფორმაციული უსაფრთხოების უწყვეტობა		
მიზანი: ინფორმაციული უსაფრთხოების უწყვეტობა ინტეგრირებული უნდა იყოს სუბიექტის საქმიანობის უწყვეტობის მართვის სისტემებში.		
17.1.1	ინფორმაციული უსაფრთხოების უწყვეტობის დაგეგმვა	*კონტროლის მექანიზმი* სუბიექტმა უნდა განსაზღვროს მოთხოვნები ინფორმაციული უსაფრთხოებისა და ინფორმაციული უსაფრთხოების უწყვეტობისადმი არასასურველ სიტუაციებში, მაგალითად, კრიზისის ან კატასტროფის დროს.
17.1.2	ინფორმაციული უსაფრთხოების უწყვეტობის დანერგვა	*კონტროლის მექანიზმი* სუბიექტმა უნდა ჩამოაყალიბოს, დოკუმენტირებულად ასახოს, დანერგოს და განახორციელოს მხარდაჭერა იმ პროცესების, პროცედურებისა და კონტროლის მექანიზმების, რომლებიც უზრუნველყოფენ ინფორმაციული უსაფრთხოების უწყვეტობას არასასურველ სიტუაციებში.
17.1.3	ინფორმაციული უსაფრთხოების უწყვეტობის შემოწმება, განხილვა და შეფასება	*კონტროლის მექანიზმი* სუბიექტმა პერიოდულად უნდა შეამოწმოს უკვე ჩამოყალიბებული და დანერგილი ინფორმაციული უსაფრთხოების უწყვეტობის კონტროლის მექანიზმები, რათა უზრუნველყოს მათი ქმედითობა და ეფექტიანობა არასასურველ სიტუაციებში.
17.2 მდგრადობა		
მიზანი: ინფორმაციის დამუშავების საშუალებების ხელმისაწვდომობის უზრუნველყოფა.		
17.2.1	ინფორმაციის დამუშავების საშუალებების ხელმისაწვდომობა	*კონტროლის მექანიზმი*

		სუბიექტმა უნდა დანერგოს ინფორმაციის დამუშავების იმგვარი საშუალებები (მათ შორის, დუბლირებული საშუალებები), რაც საჭიროა ხელმისაწვდომობის მოთხოვნების დასაკმაყოფილებლად.
18. შესაბამისობა		
18.1 საკანონმდებლო და სახელშეკრულებო მოთხოვნებთან შესაბამისობა		
მიზანი: ინფორმაციულ უსაფრთხოებასთან და ნებისმიერ უსაფრთხოების მოთხოვნებთან დაკავშირებული საკანონმდებლო, მარეგულირებელი და სახელშეკრულებო ვალდებულებების დარღვევის თავიდან არიდება.		
18.1.1	გამოსაყენებელი საკანონმდებლო ბაზისა და სახელშეკრულებო მოთხოვნების დადგენა	*კონტროლის მექანიზმი* სუბიექტმა უნდა უზრუნველყოს საკანონმდებლო და სახელშეკრულებო მოთხოვნის დასაკმაყოფილებლად მკაფიოდ განსაზღვრული ორგანიზაციული მიდგომის დოკუმენტირებული ფორმით ჩამოყალიბება და განახლება თითოეული ინფორმაციული სისტემისათვის.
18.1.2	ინტელექტუალური საკუთრების უფლებები	*კონტროლის მექანიზმი* სუბიექტმა უნდა დანერგოს ინტელექტუალურ საკუთრებასთან ან საკუთრების უფლებით დაცული პროგრამული უზრუნველყოფის გამოყენებასთან დაკავშირებული შესაბამისი პროცედურები, რათა უზრუნველყოფილ იქნეს საკანონმდებლო და სახელშეკრულებო მოთხოვნებთან შესაბამისობა.
18.1.3	ჩანაწერების დაცვა	*კონტროლის მექანიზმი* ჩანაწერები დაცული უნდა იყოს დაკარგვის, განადგურების, გაყალბების, არაავტორიზებული წვდომისა და გამოქვეყნებისგან საკანონმდებლო, სახელშეკრულებო და სუბიექტის მოთხოვნების შესაბამისად.
18.1.4	პირის მაიდენტიფიცირებელი პერსონალური ინფორმაციის დაცვა	*კონტროლის მექანიზმი* შესაბამისი საკანონმდებლო მოთხოვნების გათვალისწინებით, სუბიექტმა უნდა დაიცვას პირის მაიდენტიფიცირებელი პერსონალური ინფორმაცია.
18.1.5	კრიპტოგრაფიული კონტროლი	*კონტროლის მექანიზმი* კრიპტოგრაფიული კონტროლის მექანიზმი უნდა გამოიყენებოდეს საკანონმდებლო და სახელშეკრულებო მოთხოვნების შესაბამისად.
18.2 ინფორმაციული უსაფრთხოების განხილვა		
მიზანი: ორგანიზაციულ პოლიტიკასა და პროცედურებთან ინფორმაციული უსაფრთხოების დანერგვისა და ფუნქციონირების შესაბამისობის უზრუნველყოფა.		
18.2.1	ინფორმაციული უსაფრთხოების დამოუკიდებელი განხილვა	*კონტროლის მექანიზმი* სუბიექტის მიდგომა ინფორმაციული უსაფრთხოების მართვისა და დანერგვისადმი (მაგალითად, ინფორმაციული უსაფრთხოების კონტროლის მიზნები, კონტროლის მექანიზმები, პოლიტიკის დოკუმენტები, პროცესები და პროცედურები) უნდა იყოს დამოუკიდებლად განხილული დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებებისას.

18.2.2	უსაფრთხოების პოლიტიკების დოკუმენტებთან და სტანდარტებთან შესაბამისობა	*კონტროლის მექანიზმი* ხელმძღვანელებმა რეგულარულად უნდა განიხილონ საკუთარი პასუხისმგებლობის არეში მოქმედი ინფორმაციის დამუშავების წესების და პროცედურების შესაბამისობა უსაფრთხოების პოლიტიკის დოკუმენტებთან, სტანდარტებსა და ნებისმიერი სხვა უსაფრთხოების მოთხოვნებთან.
18.2.3	ტექნიკური შესაბამისობის შემოწმება	*კონტროლის მექანიზმი* ინფორმაციული სისტემები რეგულარულად უნდა განიხილებოდეს სუბიექტის ინფორმაციული უსაფრთხოების პოლიტიკებთან და სტანდარტებთან შესაბამისობაზე.

ამ დანართში ჩამოთვლილი კონტროლის მიზნები და მექანიზმები, შემუშავებულია სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტის - ISO 27002:2013-ის გათვალისწინებით.