ვებგვერდი, 08/04/2014
სარეგისტრაციო კოდი
120340000.22.026.016248

საქართველოს თავდაცვის მინისტრის
ბრძანება №26
2014 წლის 7 აპრილი ქ. თბილისი

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-6 პუნქტის „ბ“ ქვეპუნქტის საფუძველზე, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები.

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

საქართველოს თავდაცვის მინისტრი
ირაკლი ალასანია

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

თავი I. ზოგადი დებულებები

მუხლი 1. შესავალი

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები (შემდგომში - „მოთხოვნები“) შესასრულებლად სავალდებულოა კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის (შემდგომში - „ორგანიზაცია“).

2. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები“ თავსებადობაშია, ერთი მხრივ, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონთან, ხოლო, მეორეს მხრივ, ISO 27000 სერიის სტანდარტებთან.

მუხლი 2. ტერმინები და განმარტებები

1. ამ ბრძნებაში გამოყენებული ტერმინები და განმარტები არ უნდა განიმარტოს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით

დადგენილი ანალოგიური ტერმინებისაგან გასხვავებულად, არამედ გამოიყენება როგორც კანონით დადგენილი ტერმინების დამატებითი და დამაზუსტებელი განმარტებები.

2. ბრძანებაში გამოყენებული ტერმინებს ამ ბრძნების მიზნებისთვის აქვს შემდეგი განმარტებები:

ა) ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები - საბაზისო მოთხოვნები, სავალდებულოა შესრულდეს თანმიმდევრულად სამი წლის ვადაში ინფორმაციული უსაფრთხოების მართვის სისტემის დასანერგად;

ბ) ინფორმაციული აქტივი (შემდგომში - „აქტივი“) – ყველა ინფორმაცია და ცოდნა (კერძოდ,

ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

გ) ავტორიზებული ერთეული - ინდივიდი, სუბიექტი ან პროცესი, რომელსაც გააჩნია აქტივზე წვდომის უფლება;

დ) ხელმისაწვდომობა - ავტორიზებული სუბიექტის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი;

ე) კონფიდენციალურობა - აქტივის მახასიათებელი, რომლის თანახმადაც აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის;

ვ) მთლიანობა - აქტივის სიზუსტის და სისრულის მახასიათებელი;

ზ) ინფორმაციული უსაფრთხოება - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, აუთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

თ) ინფორმაციული უსაფრთხოების მართვის სისტემა - იუმს - მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონერება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

ი) რეაგირების გარეშე დარჩენილი რისკი - რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

კ) რისკის მიღება - გადაწყვეტილება რისკის მიღების თაობაზე;

ლ) რისკის ანალიზი - ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მის მიერ მიყენებული შესაძლო ზიანის დასადგენად;

მ) რისკის დონის დადგენა - რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

ნ) რისკების მართვა - მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

ო) რისკების მოპყრობა - რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

პ) კონტროლის მექანიზმების გამოყენებადობის განაცხადი - იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

თავი II
ორგანიზაციისათვის პირველ წელს შესასრულებელი მოთხოვნები

მუხლი 3. ორგანიზაციაში ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ხელმძღვანელობის მხრიდან მხარდაჭერა

ორგანიზაციაში უნდა არსებობდეს შიდასამსახურებრივი დოკუმენტი ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის შესახებ (იხ. დანართი 1, მგს 27001:2011, თავი 5.1 და 5.2; აგრეთვე დანართი ა-დან კონტროლი ა.6.1.1.).

მუხლი 4. ორგანიზაციული მოწყობა

ორგანიზაციამ უნდა განსაზღვროს პირი ან პირები (მაგალითად, ინფორმაციული უსაფრთხოების საბჭო, რომელიც შედგება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისაგან), რომელიც განახორციელებს ინფორმაციული უსაფრთხოების მართვას (იხ. დანართი 1, მგს 27001:2011, თავი 5.1; კონტროლები: ა.6.1.1; ა.6.1.2; ა.6.1.3.“).

მუხლი 5. გავრცელების სფერო

ორგანიზაციამ უნდა განსაზღვროს და დოკუმენტირებულად წარმოადგინოს იუმს-ის გავრცელების სფერო და საზღვრები საქმიანობის, ორგანიზაციული სტრუქტურის, ადგილმდებარეობის, აქტივებისა და ტექნოლოგიების ჭრილში, მათ შორის დაასაბუთოს დაშვებული გამონაკლისების მიზეზები და შეათანხმოს ისინი საქართველოს თავდაცვის სამინისტროსთან (შემდგომში - „სამინისტრო“) (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ა).

მუხლი 6. იუმს-ის პოლიტიკა

1. ორგანიზაციამ უნდა წარმოადგინოს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) პოლიტიკის დოკუმენტი, რომელშიც ასახული იქნება ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების მართვის სისტემის ხედვა, დასახული მიზნები და სასურველი შედეგები და დამტკიცებული იქნება ხელმძღვანელობის მიერ (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-5).

2. ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემა უნდა უზრუნველყოფდეს დაგეგმვის, დანერგვის, ფუნქციონირების, მონიტორინგისა და გაუმჯობესებისთვის საჭირო ფაზებს (იხ. დანართი 1, მგს 27001:2011, თავები: 4.1; 4.3.1ა,ბ,გ; კონტროლები: ა.5.1.1; ა.5.1.2“).

3. ინფორმაციული უსაფრთხოების პოლიტიკა:

ა) შეიცავს ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანს, ძირითად მიმართულებას და პრინციპებს (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-1);

ბ) ითვალისწინებს განაცხადს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის და სხვა სტანდარტების მოთხოვნებთან შესაბამისობის შესახებ (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-2; კონტროლი ა. 15.1);

გ) პასუხობს ორგანიზაციის რისკების მართვის კონტექსტს, რომლის ფარგლებშიც მოხდება იუმს-ის ჩამოყალიბება და მხარდაჭერა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-3).

მუხლი 7. აქტივების გამოვლენა, აღწერა, კლასიფიცირება და მართვა,

1. ორგანიზაციამ უნდა განახორციელოს დადგენილ გავრცელების სფეროში აქტივების მართვა, რაც გულისხმობს აქტივების გამოვლენის, აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და უზრუნველყოფას. (ასევე, იხ. დანართი 1, მგს 27001:2011, კონტროლები: ა.7.1 და ა.7.2 სრულად).

2. ორგანიზაციამ აქტივების მართვა უნდა განახორციელოს „ინფორმაციული აქტივების მართვის წესების შესახებ“ საქართველოს თავდაცვის მინისტრის ბრძანების შესაბამისად.

მუხლი 8. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

1. ორგანიზაციამ უნდა შეიმუშავოს და განახორციელოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ე). ორგანიზაციამ უნდა უზრუნველყოს პერსონალის კვალიფიციურობა იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

ა) იუმს-ში ჩართული პერსონალისთვის აუცილებელი ცოდნის განსაზღვრა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

გ) სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ ჩანაწერების წარმოება.

2. ორგანიზაციამ უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

თავი III
ორგანიზაციისათვის მეორე წელს შესასრულებელი მოთხოვნები

მუხლი 9. რისკების მოპყრობის გეგმა

1. ორგანიზაციამ უნდა ჩამოაყალიბოს და დანერგოს რისკების მოპყრობის გეგმა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ა-ბ), რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო ქმედებებს

ხელმძღვანელობის მხრიდან, რესურსებს (იხ. დანართი 1, მგს 27001:2011, თავი 5.2.1), პასუხისმგებლობებს და პრიორიტეტებს.

2. ორგანიზაციამ უნდა უზრუნველყოს კონტროლის მიზნების მიღწევა, რაც გულისხმობს სახსრების განაწილებას და პასუხისმგებლობების და როლების განსაზღვრას.

მუხლი 10. ორგანიზაციაში კონტროლის მექანიზმების დანერგვა

ინფორმაციული უსაფრთხოების მიზნების მისაღწევად ორგანიზაციამ უნდა:

ა) დანერგოს მეორე წლის მე-14 მუხლის მე-5 პუნქტში შერჩეული კონტროლის მექანიზმები;

ბ) კონტროლის მექანიზმების დანერგვისთანავე ორგანიზაციამ უნდა აწარმოოს მათზე დაკვირვება;

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

მუხლი 11. კონტროლის მექანიზმების ეფექტიანობის საზომების განსაზღვრა

1. ორგანიზაციამ უნდა განსაზღვროს შერჩეული კონტროლის მექანიზმების ან კონტროლის მექანიზმთა ჯგუფის ეფექტიანობის საზომები და დაადგინოს თუ როგორ და ვის მიერ მოხდება ამ საზომების გამოყენება, რათა შეფასდეს კონტროლის მექანიზმების ეფექტიანობა და მიღებული იქნას შედარებადი და განმეორებადი შედეგები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.დ).

2. კონტროლის მექანიზმის ეფექტიანობის გაზომვა ხელმძღვანელობას და პერსონალს საშუალებას აძლევს განსაზღვრონ, შერჩეული კონტროლის მექანიზმი რამდენად ეფექტიანად იძლევა კონტროლის მიზნების მიღწევის საშუალებას.

მუხლი 12. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

1. ორგანიზაციამ უნდა შეიმუშავოს და განახორციელოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ე). ორგანიზაციამ უნდა უზრუნველყოს პერსონალის კვალიფიციურობა იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

ა) იუმს-ში ჩართული პერსონალისთვის აუცილებელი ცოდნის განსაზღვრა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

გ) სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ ჩანაწერების წარმოება.

2. ორგანიზაციამ უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

მუხლი 13. იუმს-ის მონიტორინგისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა

ორგანიზაციამ უნდა დანერგოს პროცედურები და სხვა კონტროლის მექანიზმები, რაც საშუალებას მისცემს აღმოაჩინოს უსაფრთხოების შემთხვევები და რეაგირება მოახდინოს ინფორმაციული უსაფრთხოების ინციდენტებზე (იხ. დანართი 1, 27001:2011, თავი 4.2.2. თ).

მუხლი 14. რისკების მართვა

1. ორგანიზაციამ უნდა განსაზღვროს რისკების შეფასების მიდგომა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.გ);

2. ორგანიზაციამ უნდა გამოავლინოს რისკები და გაანალიზოს მათი გავლენა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.დ);

3. ორგანიზაციამ უნდა ჩაატაროს გამოვლენილი რისკების ანალიზი და შეფასება (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ე);

4. ორგანიზაციამ უნდა გამოავლინოს და შეაფასოს რისკების მოპყრობის გზები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ვ);

5. ორგანიზაციამ რისკების მოპყრობის მიზნით უნდა შეარჩიოს კონტროლის მიზნები და კონტროლის მექანიზმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ზ);

6. ორგანიზაციის ხელმძღვანელობამ უნდა დაადასტუროს ნარჩენ რისკებზე თანხმობა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.თ).

მუხლი 15. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

ორგანიზაციამ უნდა მოამზადოს კონტროლის მექანიზმების გამოყენებადობის განაცხადი (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.კ), რომელიც შეიცავს:

ა) ამ მოთხოვნების მე-8 მუხლის მე-5 პუნქტში შერჩეულ კონტროლის მიზნებს და კონტროლის მექანიზმებს, ასევე მათი შერჩევის დასაბუთებას;

ბ) ორგანიზაციაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

გ) მგს 27001:2011-ის დანართი ა-დან ნებისმიერი გამორიცხული კონტროლის მიზნის და კონტროლის მექანიზმების ჩამონათვალს და გამორიცხვის დასაბუთებას.

მუხლი 16. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა

1. ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის უახლესი ვერსიის ხელმისაწვდომობა ყველა უფლებამოსილი პირისთვის, ასევე იუმს-ის დოკუმენტაცის სათანადოდ დაცვა და კონტროლი (იხ. დანართი 1, მგს 27001:2011 თავი 4.3.2.).

2. ორგანიზაციამ უნდა აწარმოოს ჩანაწერები და უზრუნველყოს მათი მხარდაჭერა იუმს-ის მოთხოვნებთან შესაბამისობისა და ეფექტიანი ფუნქციონირების მიზნით. ჩანაწერები უნდა იყოს სათანადოდ დაცული და კონტროლდებოდეს (იხ. მგს 27001:2011 თავი 4.3.3).

3. ორგანიზაციის იუმს-ის დოკუმენტაცია მოიცავს (იხ. მგს 27001:2011 თავი 4.3.1):

ა) იუმს-ის პოლიტიკას;

ბ) იუმს-ის გავრცელების სფეროს;

გ) იუმს-ის მხარდამჭერ პროცედურებსა და კონტროლებს;

დ) რისკების შეფასების მეთოდოლოგიის აღწერას;

ე) რისკების შეფასების ანგარიშს;

ვ) რისკების მოპყრობის გეგმას (არ არის სავალდებულო პირველ წელს);

ზ) კონტროლის მექანიზმების ეფექტიანობის საზომების აღწერას (არ არის სავალდებულო პირველ წელს);

თ) ჩანაწერებს;

ი) კონტროლის მექანიზმების გამოყენებადობის განაცხადს.

თავი IV
ორგანიზაციისათვის მესამე წელს შესასრულებელი მოთხოვნები

მუხლი 17. მონიტორინგი

1. ორგანიზაციამ უნდა დანერგოს და განახორციელოს მონიტორინგის და განხილვის პროცედურები, ასევე სხვა კონტროლის მექანიზმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ა), რომელთა მიზანია:

ა) დამუშავების შედეგებში შეცდომების მყისიერი აღმოჩენა;

ბ) უსაფრთხოების გარღვევის მცდელობების და წარმატებული მცდელობების, აგრეთვე ინციდენტების მყისიერი აღმოჩენა;

გ) მიეცეს ხელმძღვანელობას მსჯელობის საშუალება, თუ რამდენად ეფექტიანად მუშაობს უსაფრთხოების ესა თუ ის ღონისძიება;

დ) გამოავლინოს უსაფრთხოების შემთხვევების ინდიკატორების მეშვეობით;

ე) განსაზღვროს, იყო თუ არა გარღვევის მცდელობის აღმოფხვრა ეფექტიანი.

2. ორგანიზაციამ პერიოდულად უნდა განიხილოს იუმს-ის ეფექტიანობა (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვა). პერიოდული მიმოხილვის დროს ორგანიზაციამ უნდა გაითვალისწინოს ინფორმაციული უსაფრთხოების აუდიტის შედეგები, ინციდენტები, ეფექტიანობის გაზომვის შედეგები და დაინტერესებული მხარეებისგან მიღებული შემოთავაზებები და უკუკავშირი (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ბ).

3. ორგანიზაციამ უნდა გაზომოს კონტროლის მექანიზმების ეფექტიანობა უსაფრთხოების მოთხოვნების დაკმაყოფილების დასადასტურებლად (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.გ).

მუხლი 18. რისკების შეფასების გადახედვა

ორგანიზაციამ დაგეგმილი პერიოდულობით უნდა განახორციელოს რისკების შეფასების, ნარჩენი რისკებისა და რისკების მისაღები დონეების გადახედვა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.დ), შემდეგი საკითხების გათვალისწინებით:

ა) ორგანიზაციულ-სტრუქტურული ცვლილება;

ბ) ტექნოლოგიური ცვლილება;

გ) ცვლილება საქმიანობის მიზნებსა და პროცესებში;

დ) ახლადაღმოჩენილი საფრთხეები;

ე) დანერგილი კონტროლის მექანიზმების ეფექტიანობის ცვლილება;

ვ) გარე მოვლენები, ისეთი როგორიცაა საკანონმდებლო ცვლილებები;

ზ) შეცვლილი საკონტრაქტო ვალდებულებები და ცვლილებები სოციალურ გარემოში;

მუხლი 19. ორგანიზაციაში იუმს-ის შიდა აუდიტი

1. ორგანიზაცია ვალდებულია ჩაატაროს იუმს-ის აუდიტი (იხ. დანართი 1, მგს 27001:2011 თავი 6) დაგეგმილი პერიოდულობით და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები:

ა) შეესაბამება თუ არა სტანდარტის, საკანონმდებლო მოთხოვნებს;

ბ) შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება თუ არა მისი დანერგვა და მხარდაჭერა;

დ) ფუნქციონირებს თუ არა გეგმის შესაბამისად.

2. ხელმძღვანელობას, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და მათი გამომწვევი მიზეზების აღმოფხვრა. შემდგომი ღონისძიებები გულისხმობს მათ შემოწმებას და შემოწმების შედეგების ანგარიშგებას (იხ. დანართი 1, მგს 27001:2011 თავი 8).

მუხლი 20. ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა

1. ორგანიზაციამ უნდა განახორციელოს იუმს-ის პერიოდული მიმოხილვა, რათა უზრუნველყოფილი იყოს ადეკვატური გავრცელების სფერო და იუმს-ს პროცესის გაუმჯობესებების აღმოჩენა (იხ. დანართი 1, მგს 27001:2011, თავი 7).

2. ხელმძღვანელობა ვალდებულია აწარმოოს იუმს-ს მიმოხილვა დაგეგმილი პერიოდულობით (სულ მცირე წელიწადში ერთხელ) მუდმივი შესაბამისობის, ადექვატურობისა და ეფექტიანობის უზრუნველსაყოფად. მიმოხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვილებების საჭიროებას, მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკას და მიზნებს.

3. მიმოხილვის შედეგები უნდა იყოს დოკუმენტირებული და ხდებოდეს ჩანაწერების წარმოება (იხ. დანართი 1, მგს 27001:2011 თავი 4.3.3).

მუხლი 21. ინფორმაციული უსაფრთხოების ღონისძიებების გეგმების განახლება

ორგანიზაციამ მონიტორინგის და მიმოხილვის შედეგების გათვალისწინებით უნდა განაახლოს ინფორმაციული უსაფრთხოების ღონისძიებების გეგმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ზ).

მუხლი 22. ორგანიზაციაში იუმს-ის გაუმჯობესება და კომუნიკაცია

ორგანიზაცია ვალდებულია:

ა) იუმს-ში დანერგოს გამოვლენილი გაუმჯობესებები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.4.ა);

ბ) განახორციელოს ყველა დაინტერესებული პირის ინფორმირება გატარებული ქმედებების და გაუმჯობესებების თაობაზე დეტალიზაციის შესაბამისი დონის გათვალისწინებით და, საჭიროების შემთხვევაში, შეათანხმოს შემდგომი ნაბიჯები ინფორმაციული უსაფრთხოების მართვის სისტემაზე პასუხისმგებელ პირებთან (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.4.გ;).

მუხლი 23. იუმს-ის მხარდაჭერა

1. ორგანიზაცია ვალდებულია მუდმივად იზრუნოს იუმს-ის ეფექტიანობის გაუმჯობესებაზე შემდეგი საკითხების გათვალისწინებით:

ა) ინფორმაციული უსაფრთხოების პოლიტიკა და ინფორმაციული უსაფრთხოების მიზნები;

ბ) აუდიტის შედეგები;

გ) მონიტორინგის შედეგად აღმოჩენილი მოვლენების ანალიზი, მაკორექტირებელი და პრევენციული ქმედებები;

დ) ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა (იხ. დანართი 1, მგს 27001:2011 თავი 7).

2. ორგანიზაციამ უნდა:

ა) განახორციელოს მგს 27001:2011-ის 8.2-სა და 8.3-ის თანახმად შესაბამისი მაკორექტირებელი და პრევენციული ქმედებები;

ბ) უზრუნველყოს გაუმჯობესებების შედეგად დასახული მიზნების მიღწევა.

დანართი № 1

მგს 27001:2011
ინფორმაციული ტექნოლოგიები - უსაფრთხოების საშუალებები - ინფორმაციული უსაფრთხოების მართვის სისტემები - მოთხოვნები

შესავალი

წინამდებარე სტანდარტის მიზანი არის ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში „იუმს“) ჩამოყალიბება, დანერგვა, ფუნქციონირება, ზედამხედველობა, მხარდაჭერა და გაუმჯობესება. იუმს-ის ორგანიზაციაში მიღება სტრატეგიული გადაწყვეტილება უნდა იყოს. ორგანიზაციაში იუმს-ის დიზაინი და დანერგვა განპირობებულია ორგანიზაციის საჭიროებებით და მიზნებით, უსაფრთხოების მოთხოვნებით, არსებული პროცესებით და ორგანიზაციული სტრუქტურით, რომლებიც შესაძლოა დროთა განმავლობაში იცვლებოდეს. მოსალოდნელია, რომ იუმს-ის დანერგვა შეიცვლება ორგანიზაციის საჭიროებების

მიხედვით. სტანდარტი შესაძლოა გამოყენებულ იქნეს შესაბამისობის შესამოწმებლად შიდა და გარე დაინტერესებული პირების მიერ.

1. გავრცელების სფერო

1.1.ზოგადი

წინამდებარე სტანდარტი ვრცელდება კრიტიკული ინფორმაციული სისტემის მქონე სუბიექტებზე (შემდეგში '"ორგანიზაციაზე"). სტანდარტი განსაზღვრავს იუმს-ის ჩამოყალიბების, დანერგვის, ფუნქციონიონირების, მონიტორინგის, განხილვის, მხარდაჭერისა და გაუმჯობესების დოკუმენტირებულ მოთხოვნებს ორგანიზაციაში არსებული ზოგადი ბიზნეს-რისკების გათვალისწინებით.

სტანდარტი აღწერს უსაფრთხოების კონტროლის მექანიზმების დანერგვის მოთხოვნებს ყოველი კონკრეტული ორგანიზაციისათვის, ან მისი ნაწილისათვის. იუმს-ის დანიშნულებაა ინფორმაციული აქტივების დამცავი, ადეკვატური და პროპორციული უსაფრთხოების კონტროლის მექანიზმების დანერგვა და დაინტერესებული მხარეების დარწმუნებულობის გამყარება.

შენიშვნა 1: „ბიზნესის" გამოყენება სტანდარტში უნდა განიხილებოდეს, როგორც ძირითად საქმიანობათა ერთობლიობა, რომელიც აუცილებელია ორგანიზაციის არსებობისათვის.

შენიშვნა 2: სტანდარტი წარმოადგენს დანერგვის სახელმძღვანელოს, რომელიც შესაძლოა გამოყენებულ იქნეს კონტროლის მექანიზმის დიზაინის სტადიაზე.

1.2.გამოყენება

სტანდარტში ჩამოყალიბებული მოთხოვნები არის ზოგადი და უნდა გამოიყენებოდეს ორგანიზაციაში, მიუხედავად მისი სიდიდის, ზომის და ტიპისა. იმისათვის, რომ ორგანიზაცია თავსებადობაში იყოს აღნიშნულ სტანდარტთან, არ დაიშვება 4, 5, 6, 7 და 8 პუნქტებში ჩამოთვლილი არცერთი მოთხოვნის ამოღება. ნებისმიერი კონტროლის მექანიზმის ამოღება, რომელიც აუცილებელია რისკის მისაღებად, უნდა იყოს დაფიქსირებული და გააზრებული და უნდა არსებობდეს მტკიცებულება იმისა, რომ შესაბამისი რისკები მიღებულია პასუხისმგებელი პირების მიერ. სტანდარტთან შესაბამისობა შეუძლებელია, თუ რომელიმე მოთხოვნა ამოღებული იქნება, გარდა იმ შემთხვევებისა, როდესაც ასეთი გამონაკლისები პირდაპირ არის საკანონმდებლო ან მარეგულირებელ ბაზასთან წინააღმდეგობაში, ან უარყოფითად მოქმედებს ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების მიწოდების შესაძლებლობაზე.

შენიშვნა: იმ შემთხვევაში, როდესაც ორგანიზაციას უკვე გააჩნია ბიზნეს-პროცესის მართვის სისტემა (მაგ. ხარისხის მართვის სისტემები ISO 9001 ან გარემოს მართვის სისტემა ISO 14001), უმეტეს შემთხვევაში სასურველია შესაბამისობა წინამდებარე სტანდარტთან მართვის არსებული სისტემის ფარგლებში.

2. ნორმატიული აქტები

დოკუმენტში დასახელებული სხვა დოკუმენტები წარმოადგენს წინამდებარე სტანდარტის განუყოფელ ნაწილს.

3. ტერმინები და განმარტებები

შენიშვნა: დოკუმენტის ამ ნაწილში მოყვანილი ტერმინები და განმარტებები არ უნდა განიმარტოს „ინფორმაციული უსაფრთხოების შესახებ“ კანონით დადგენილი ანალოგიური ტერმინებისაგან გასხვავებულად, არამედ გამოიყენება როგორც კანონით დადგენილი ტერმინების დამატებითი და დამაზუსტებელი განმარტებები.

3.1.აქტივი

ნებისმიერი რამ, რაც ფასეულია ორგანიზაციისათვის;

3.2.ხელმისაწვდომობა

ავტორიზებული სუბიექტის მიერ მოთხოვნის შესაბამისად ხელმისაწვდომობისა და გამოყენებადობის მახასიათებლები.

3.3.კონფიდენციალურობა

მახასიათებლები იმისა, რომ ინფორმაცია არ არის ხელმისაწვდომი არაავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის;

3.4.ინფორმაციული უსაფრთხოება

ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შენარჩუნება და დაცვა; დამატებით შესაძლოა მოიცავდეს ასევე ისეთ მახასიათებლებს, როგორებიცაა: ავთენტურობა, ანგარიშვალდებულება, წარმოშობის წყაროსთან ცალსახა შესაბამისობა და სანდოობა;

3.5.ინფორმაციული უსაფრთხოების მოვლენა

სისტემის, სერვისისა და ქსელის იდენტიფიცირებული მდგომარეობა, რაც მიუთითებს ინფორმაციული უსაფრთხოების პოლიტიკის შესაძლო დარღვევაზე ან დანერგილი კონტროლის მექანიზმების წარუმატებლობაზე, ან წინასწარ უცნობ ისეთ სიტუაციაზე, რომელიც შესაძლოა მნიშვნელოვანი იყოს უსაფრთხოების თვალსაზრისით;

3.6.ინფორმაციული უსაფრთხოების ინციდენტი

ინფორმაციული უსაფრთხოების მოულოდნელი ან არასასურველი ცალკეული ან სერიული ხდომილებები, რომლებიც დიდი ალბათობით ახდენენ ბიზნეს-ოპერაციების დისკრედიტაციას ან ემუქრებიან ინფორმაციულ უსაფრთხოებას;

3.7. ინფორმაციული უსაფრთხოების მართვის სისტემა - იუმს

მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

3.8 მთლიანობა

აქტივის სიზუსტის და სრულყოფილების დაცვის მახასიათებელი თვისება;

3.9 რეაგირების გარეშე დარჩენილი რისკი

რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

3.10. რისკის მიღება

გადაწყვეტილება რისკის მიღების თაობაზე;

3.11. რისკის ანალიზი

ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მისი შეფასების დასადგენად;

3.12. რისკის შეფასება

რისკის ანალიზისა და რისკის დონის დადგენის სრული პროცესი;

3.13. რისკის დონის დადგენა

რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

3.14. რისკის მართვა

ორგანიზაციის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

3.15. რისკების მოპყრობა

რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

3.16. გამოყენებადობის შესახებ განაცხადი

ორგანიზაციის იუმს-ისთვის საჭირო და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

4. ინფორმაციული უსაფრთხოების მართვის სისტემა

4.1.ზოგადი მოთხოვნები

ორგანიზაციამ უნდა ჩამოაყალიბოს

ორგანიზაციამ უნდა ჩამოაყალიბოს, დანერგოს, გამოიყენოს, განახორციელოს მონიტორინგი, განიხილოს, მხარი დაუჭიროს და გააუმჯობესოს დოკუმენტირებული იუმს ორგანიზაციაში ასრებული ყველა ბიზნეს-პროცესის და რისკების გათვალისწინებით. ამ სტანდარტის მიზნებისთვის გამოიყენება „დაგეგმვა-აღსრულება-შემოწმება-ქმედება“ მოდელი, რომელიც ნაჩვენებია ნახაზზე.

4.2. იუმს-ის ჩამოყალიბება და მართვა

4.2.1.იუმს-ის ჩამოყალიბება

ორგანიზაციამ უნდა შეასრულოს შემდეგი:

ა) განსაზღვროს იუმს-ის გავრცელების სფერო და საზღვრები ბიზნესის, ორგანიზაციის, ადგილმდებარეობის, აქტივების და ტექნოლოგიების ჭრილში, მათ შორის დაასაბუთოს დაშვებული გამონაკლისების მიზეზები (იხილეთ პუნქტი 1.2.)

ბ) განსაზღვროს იუმს პოლიტიკა ბიზნესის, ორგანიზაციის, ადგილმდებარეობის, აქტივების და ტექნოლოგიების ჭრილში, რომელიც:

1. ინფორმაციულ უსაფრთხოებასთან მიმართებაში აყალიბებს მიზნებს, საერთო მიმართულებას და პრინციპებს;

2. ითვალისწინებს საკანონმდებლო და ბიზნესის მარეგულირებელ მოთხოვნებს, აგრეთვე საკონტრაქტო მოთხოვნებს;

3. შეესაბამება ორგანიზაციის სტრატეგიული რისკების მართვის კონტექსტს, რომელშიც მოხდება იუმს-ის ჩამოყალიბება და შენარჩუნება;

4. აყალიბებს რისკების შეფასების კრიტერიუმებს;

5. დამტკიცებულია მენეჯმენტის მიერ.

შენიშვნა: წინამდებარე სტანდარტის მიზნებიდან გამომდინარე იუმს პოლიტიკა განიხილება, როგორც ინფორმაციული უსაფრთხოების პოლიტიკის მომცველი. თუმცა, ეს პოლიტიკები შესაძლოა ერთ დოკუმენტად იყოს ჩამოყალიბებული.

გ) განისაზღვროს ორგანიზაციის რისკების შეფასების მიდგომა.

1. ჩამოყალიბდეს რისკების შეფასების მეთოდოლოგია, რომელიც შესაბმისობაში იქნება იუმს-თან და გაითვალისწინებს ბიზნესის ინფორმაციული უსაფრთხოების, საკანონმდებლო და მარეგულირებელ მოთხოვნებს.

2. შემუშავდეს რისკების მიღების კრიტერიუმები და განისაზღვროს დასაშვები რისკის დონეები.

რისკების შეფასების შერჩეულმა მეთოდოლოგიამ უნდა უზრუნველყოს რისკების შეფასების შედარებადი და განმეორებადი შედეგები.

შენიშვნა: არსებობს რისკების შეფასების სხვადასხვა მეთოდოლოგია. მაგალითები მოყვანილია დოკუმენტში ISO/IEC TR 13335-3, Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security.

დ) გამოვლინდეს რისკები:

1. გამოვლინდეს იუმს-ის ფარგლებში აქტივები და მათი მფლობელები*;

2. გამოვლინდეს ამ აქტივებთან დაკავშირებული საფრთხეები;

3. გამოვლინდეს სისუსტეები, რომელებითაც შესაძლოა ისარგებლონ საფრთხეებმა;

4.გამოვლინდეს აქტივებზე კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევით გამოწვეული დანაკარგები.

შენიშვნა: ტერმინი „მფლობელი“ გამოიყენება ინდივიდის ან ობიექტის აღსაწერად, რომელსაც გააჩნია აქტივის წარმოების, შენარჩუნების ან დაცვის მოვალეობა. „მფლობელი“ არ ნიშნავს იმას, რომ პიროვნებას გააჩნია აქტივზე საკუთრების უფლება.

ე) გააანალიზოს და შეაფასოს რისკები.

1. შეფასდეს ორგანიზაციის ბიზნესისთვის უსაფრთხოების დარღვევით გამოწვეული შედეგი კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევის გათვალისწინებით;

2. შეფასდეს უსაფთხოების დარღვევის ხდომილების ალბათობა ჭარბი საფრთხეების და სისუსტეების შემთხვევაში, აქტივებზე მათი შედეგები და არსებული კონტროლის მექანიზმები.

3. შეფასდეს რისკის დონეები.

4. განისაზღვროს, მოხდება თუ არა რისკის მიღება და საჭიროებს თუ არა რისკი მოპყრობას რისკების მიღების კრიტერიუმების შესაბამისად (იხ.4.2.1გ)2).

ვ) აღმოჩენილ იქნეს და შეფასდეს რისკების მიღების ნაირსახეობები. შესაძლო ქმედებები არის:

1. შესაბამისი კონტროლის მექანიზმების გამოყენება;

2. გაცნობიერებულად და ობიექტურად რისკის მიღება ორგანიზაციის პოლიტიკების და რისკების მიღების კრიტერიუმების გათვალისწინებით;

3. რისკის თავიდან აცილება.

4. რისკის გადატანა სხვა მხარეებზე, მაგალითად დაზღვევა, მომწოდებლები.

ზ) რისკების სამართავად უნდა მოხდეს კონტროლის მიზნების და კონტროლის მექანიზმების შერჩევა, რომელიც უნდა შეესაბამებოდეს რისკების შეფასების და რისკების მოპყრობის პროცესს. შერჩევა უნდა ეფუძნებოდეს რისკების მიღების კრიტერიუმებს (იხ 4.2.1 გ)2)), აგრეთვე საკანონმდებლო, მარეგულირებელ და საკონტრაქტო მოთხოვნებს.

დანართში ა მოცემული კონტროლის მიზნები და კონტროლის მექანიზმები უნდა იყოს ამ პროცესის შემადგენელი. თუმცა, დანართში ა მოცემული კონტროლის მექანიზმები და კონტროლის მიზნები არ წარმოადგენს ამომწურავ ჩამონათვალს, ამიტომ შესაძლებელია შეირჩეს დამატებითი კონტროლის მექანიზმები.

შენიშვნა: დანართი ა წარმოადგენს კონტროლის მექანიზმების და კონტროლის მიზნების ზოგად ჩამონათვალს. წინამდებარე სტანდარტის მომხმარებლები განიხილავენ დანართ ა-ს კონტროლის მექანიზმების შერჩევის საწყის წერტილად, რათა არ მოხდეს მნიშვნელოვანი კონრტოლის მექანიზმების გამოტოვება.

თ) რეაგირების გარეშე დარჩენილი რისკების შესახებ მენეჯმენტისგან თანხმობის მიღება.

ი) იუმს-ის დანერგვასა და ფუნქციონირების თაობაზე მენეჯმენტისგან თანხმობის მიღება.

კ) გამოყენებადობის შესახებ განაცხადი უნდა მომზადდეს და ძირითადად უნდა შეიცავდეს:

1. კონტროლის მიზნებს და 4.2.1თ) -ში შერჩეულ კონტროლის მექანიზმებს და მათი შერჩევის მიზეზებს;

2. არსებული კონტროლების მიზნებს და კონტროლის მექანიზმებს (იხ.4.2.1 ე)2);

3. ნებისმიერი კონტროლის მიზნების და კონტროლის მექანიზმების ამოღებას დანართი ა-დან და ამოღების დასაბუთებას.

შენიშვნა: გამოყენებადობის შესახებ განაცხადი წარმოადგენს გადაწყვეტილებათა შეჯამებას რისკებთან მოპყრობის შესახებ. გამონაკლისების ახსნა კიდევ ერთი შემოწმების საშუალებაა იმისა, რომ არაფერი გამოგვრჩა მნიშვნელოვანი.

4.2.2.იუმს-ის დანერგვა და ფუნქციონირება

ორგანიზაციამ უნდა შეასრულოს შემდეგი:

ა) ჩამოაყალიბოს რისკთან მოპყრობის გეგმა, რომელიც აღწერს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო მენეჯმენტის ქმედებებს, რესურსებს, პასუხისმგებლობებს და პრიორიტეტებს (იხილეთ პუნქტი 5).

ბ) დანერგოს რისკების მოპყრობის გეგმა, რათა მოხდეს კონტროლის მიზნების მიღწევა, რაც გულისხმობს სახსრების განაწილებას და პასუხისმგებლობების და როლების განსაზღვრას.

გ) დაინერგოს 4.2.1 ზ-ში ნახსენები კონტროლის მექანიზმები, რათა მოხდეს კონტროლის მიზნების მიღწევა.

დ) განისაზღვროს შერჩეული კონტროლის მექანიზმების ან კონტროლის მექანიზმების ჯგუფის ეფექტიანობის გაზომვის საშუალებები და დადგინდეს თუ როგორ მოხდება ამ საზომების გამოყენება (4.2.3გ).

შენიშვნა: კონტროლის მექანიზმის ეფექტიანობის გაზომვა მენეჯერებს და პერსონალს საშუალებას აძლევს განსაზღვრონ, შერჩეული კონტროლის მექანიზმი რამდენად ეფექტიანად იძლევა კონტროლის მიზნების მიღწევის საშუალებას.

ე) დაინერგოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხილეთ 5.2.2.);

ვ) მართოს იუმს ფუნქციონირება;

ზ) მართოს იუმს რესურსები (იხილეთ 5.2);

თ) დანერგოს პროცედურები და სხვა კონტროლის მექანიზმები, რომლებიც დაეხმარება უსაფრთხოების მოვლენების აღმოჩენაში და ამ ინციდენტებზე რეაგირებაში (იხილეთ 4.2.3. ა)).

4.2.3.იუმს-ის მონიტორინგი და განხილვა

ორგანიზაცია ვალდებულია:

ა) განახორციელოს მონიტორინგი და განხილვის პროცედურები და სხვა კონტროლის მექანიზმები, რათა:

1. დამუშავების შედეგებში დაუყოვნებლივ აღმოაჩინოს შეცდომები;

2. დაუყოვნებლივ აღმოაჩინოს უსაფრთხოების გარღვევის მცდელობები, ინციდენტები და შედეგები;

3. მისცეს მენეჯმენტს მსჯელობის საშუალება, თუ რამდენად ეფექტიანად მუშაობს ესა თუ ის უსაფრთხოების კონტროლის მექანიზმები;

4. დაეხმაროს უსაფრთხოების მოვლენების აღმოჩენაში და ინდიკატორების მეშვეობით უსაფრთხოების ინციდენტების თავიდან აცილებაში;

5. განსაზღვროს, იყო თუ არა გარღვევის მცდელობის აღმოფხვრა შედეგიანი.

ბ) აწარმოოს იუმს ეფექტიანობის პერიოდული მიმოხილვა (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვა) უსაფრთხოების აუდიტების, ინციდენტების, ეფექტიანობის გაზომვის შედეგების გათვალისწინებით და დაინტერესებული მხარეებისგან შემოთავაზებების და უკუკავშირის გათვალისწინებით.

გ) გაზომოს კონტროლის მექანიზმების ეფექტიანობა უსაფრთხოების მოთხოვნების დაკმაყოფილების შესამოწმებლად;

დ) განახორციელოს რისკების შეფასების განხილვა დროის დაგეგმილ ინტერვალებში, რეაგირების გარეშე დარჩენილი რისკების და რისკების მისაღები დონის განხილვა, შემდეგი ცვლილებების გათვალისწინებით:

1. ორგანიზაცია;

2. ტექნოლოგია;

3. ბიზნესის მიზნები და პროცესები;

4. აღმოჩენილი საფრთხეები;

5. დანერგილი კონტროლის მექანიზმების ეფექტიანობა;

6. გარე მოვლენები, ისეთი როგორც საკანონმდებლო და მარეგულირებელი ცვლილებები, შეცვლილი საკონტრაქტო ვალდებულებები და ცვლილებები სოციალურ გარემოში;

ე) განხორციელდეს იუმს-ის პერიოდული აუდიტები (იხილეთ პუნქტი 6).

შენიშვნა: შიდა აუდიტების განხორციელება ხდება ორგანიზაციის მიერ ან ორგანიზაციის სახელით, შიდა მიზნებიდან გამომდინარე.

ვ) განხორციელდეს იუმს-ის პერიოდული განხილვა, რათა უზურნველყოფილი იყოს ადექვატური გავრცელების სფერო და იუმს-ის პროცესის გაუმჯობესებების აღმოჩენა (იხ 7.1);

ზ) განაახლოს უსაფრთხოების გეგმები მონიტორინგის დაკვირვებების და განხილვის შედეგების გათვალისწინებით;

თ) ქმედებების და მოვლენების დაფიქსირება, რომლებმაც შეიძლება გავლენა იქონიოს იუმს-ის ეფექტიანობაზე ან წარმადობაზე (იხ. 4.3.3).

4.2.4.იუმს-ის შენარჩუნება და გაუმჯობესება

ორგანიზაცია ვალდებულია პერიოდულად განახორციელოს:

ა) აღმოჩენილი გაუმჯობესების იუმს-ში დანერგვა;

ბ) 8.2 და 8.3 თანახმად განახორციელოს შესაბამისი მაკორექტირებელი და პრევენციული ქმედებები. გამოიყენოს სხვა ორგანიზაციების და საკუთარი გამოცდილება ამ საკითხში.

გ) მოახდინოს ყველა დაინტერესებული პირის შეტყობინება განხორციელებული ქმედებების და გაუმჯობესებების თაობაზე ვითარების შესაბამისი დეტალიზაციის დონის გათვალისწინებით და შეათანხმოს შემდგომი ნაბიჯები.

დ) უზრუნველყოს დაგეგმილი მიზნების რეალიზაცია გაუმჯობესებების მეშვეობით.

4.3.დოკუმენტაციის მოთხოვნები

4.3.1.ზოგადი

დოკუმენტაცია უნდა შეიცავდეს ჩანაწერებს მენეჯერული გადაწყვეტილებების შესახებ, უზრუნველყოს მოქმედებების ცალსახა იდენტიფიცირება მენეჯერულ გადაწყვეტილებებთან და პოლიტიკებთან და უზრუნველყოს დაფიქსირებული შედეგების განმეორებადობა. მნიშვნელოვანია ურთიერთკავშირის დამყარება შერჩეულ კონტროლის მექანიზმებსა და რისკების შეფასების და რისკების მოპყრობის პროცესებს შორის, აგრეთვე იუმს პოლიტიკასა და მიზნებთან. იუმს დოკუმენტაცია უნდა შეიცავდეს:

ა) იუმს-ის პოლიტიკის დოკუმენტირებულ ფორმულირებას (4.2.1 ბ) და მიზნებს;

ბ) იუმს-ის გავრცელების სფეროს (4.2.1 ა);

გ) იუმს-ის მხარდამჭერ პროცედურებსა და კონტროლის მექანიზმებს;

დ) რისკების შეფასების მეთოდოლოგიის აღწერას (4.2.1 გ);

ე) რისკების შეფასების ანგარიშს (4.2.1 გ-დან 4.2.1 ზ-მდე);

ვ) რისკების მოპყრობის გეგმას (4.2.2 ბ);

ზ) უსაფრთხოების პოლიტიკის პროცესების ეფექტიანი დაგეგმარებისა, ფუნქციონირების და კონტროლისათვის აუცილებელ ორგანიზაციულ დოკუმენტირებულ პროცედურებს და აღიწეროს, თუ როგორ უნდა განხორციელდეს კონტროლის მექანიზმების ეფექტიანობის გაზომვა (4.2.3 გ);

თ) წინამდებარე სტანდარტით აუცილებელ ჩანაწერებს (4.3.3);

ი) გამოყენებადობის შესახებ განაცხადს.

შენიშვნა 1: ტერმინი „დოკუმენტირებული პროცედურა“ გამოიყენება წინამდებარე სტანდარტში, ნიშნავს, რომ პროცედურა არის ჩამოყალიბებული, დოკუმენტირებული, დანერგილი და მხარდაჭერილი.

შენიშვნა 2: იუმს დოკუმენტაციის დაწვრილმანება შესაძლოა ვარირებდეს სხვადასხვა ორგანიზაციაში შემდეგის გათვალისწინებით:

• ორგანიზაციის სიდიდე და მისი საქმიანობის ტიპი;

• უსაფრთხოების მოთხოვნების და მართვის სისტემის გავრცელების სფერო და სირთულე;

შენიშვნა 3: დოკუმენტები და ჩანაწერები შესაძლოა იყოს ინფორმაციის ნებისმიერი სახის ან ტიპის მატარებელზე.

4.3.2.დოკუმენტებზე კონტროლი

იუმს-ის მიერ მოთხოვნილი დოკუმენტები უნდა იყოს დაცული. ჩამოსაყალიბებელი დოკუმენტირებული პროცედურა განისაზღვრავს მენეჯმენტის შემდეგ ქმედებებს:

ა) დოკუმენტის გამოქვეყნებამდე მისი დადასტურება;

ბ) დოკუმენტების განხილვა და ცვლილება აუცილებლობის შემთხვევაში და მისი თავიდან დადასტურება;

გ) უზრუნველყოს დოკუმენტების მიმდინარე ვერსიისა და ცვლილებების დაფიქსირება;

დ) უზრუნველყოს დოკუმენტის სხვადასხვა ვერსიების ხელმისაწვდომობა საჭიროების შემთხვევაში;

ე) უზრუნველყოს, რომ დოკუმენტები არის ჩამოყალიბებული მკაფიოდ და ცალსახად იდენტიფიცირებადია;

ვ) უზრუნლველყოს დოკუმენტების ხელმისაწვდომობა ყველა უფლებამოსილი მხარისათვის და მათი გადაადგილების, შენახვის და განადგურების არსებულ კლასიფიცირების პროცედურებთან შესაბამისობა.

ზ) უზრუნველყოს გარე წარმოშობის დოკუმენტების იდენტიფიცირება;

თ) უზრუნველყოს დოკუმენტების განაწილებაზე კონტროლი;

ი) აიკრძალოს ძველი დოკუმენტების არასათანადოდ გამოყენება, და;

კ) ნებისმიერი მიზნით შენახვის შემთხვევაში გამოიყენებოდეს სათანადო იდენტიფიცირება;

4.3.3. ჩანაწერთა კონტროლი

ჩანაწერები უნდა შეიქმნას და შენარჩუნდეს, რათა უზრუნველყოფილი იყოს იუმს-ის მოთხოვნებთან შესაბამისობა და ეფექტიანი ფუნქციონირება. ჩანაწერები უნდა იყოს დაცული და კონტროლდებოდეს. იუმს-მა უნდა გაითვალისწინოს ნებისმიერი საკანონმდებლო, მარეგულირებელი ან სახელშეკრულებო ვალდებულება. ჩანაწერები უნდა იყოს მკაფიო, იდენტიფიცირებადი და ხელმისაწვდომი. იდენტიფიცირების, შენახვის, დაცვის, ხელმისაწვდომობის, განადგურების ვადის და განთავსებისთვის საჭირო კონტროლის მექანიზმები უნდა იყოს აღწერილი და დანერგილი. პროცესის წარმადობის და იუმს-ის ყველა უსაფრთხოების ინციდენტის შესახებ ჩანაწერების შენახვა უნდა მოხდეს 4.2-ს მიხედვით.

მაგალითი: ჩანაწერთა მაგალითი შესაძლოა იყოს ვიზიტორების სარეგისტრაციო ჟურნალი, აუდიტის ანგარიში და წვდომის დაშვების ფორმა.

5. მენეჯმენტის პასუხისმგებლობა

5.1. მენეჯმენტის მზადყოფნა

მენეჯმენტი ვალდებულია წარადგინოს მზადყოფნის შესახებ მტკიცებულება იუმს-ის ჩამოყალიბებაზე, დანერგვაზე, ფუნქციონირებაზე, მონიტორინგზე, განხილვაზე, შენარჩუნებაზე და გაუმჯობესებაზე შემდეგი ჩამონათვლის გათვალისწინებით:

ა) იუმს პოლიტიკის ჩამოყალიბებით;

ბ) იუმს მიზნების და გეგმების ჩამოყალიბებით;

გ) ინფორმაციული უსაფრთხოების როლების და პასუხისმგებლობების ჩამოყალიბებით;

დ) ორგანიზაციისადმი ინფორმაციული უსაფრთხოების მიზნების და პოლიტიკის მნიშვნელობის, მისი საკანონმდებლო პასუხისმგებლობის და მუდმივი გაუმჯობესების აუცილებლობის ახსნით;

ე) იუმს-ის ჩამოსაყალიბებლად, დასანერგად, ფუნქციონირებისათვის, მონიტორინგისათვის, შენარჩუნებისათვის, განხილვისათვის და გაუმჯობესებისათვის საკმარისი რესურსების გამოყოფა (იხილეთ 5.2.1);

ვ) განსაზღვროს რისკის მიღების და დასაშვები რისკის დონეების კრიტერიუმები;

ზ) უზრუნველყოს იუმს-ის შიდა აუდიტების წარმოება (იხ.6);

თ) მოახდინოს იუმს-ის მენეჯერული განხილვა (იხ.7).

5.2. რესურსების მართვა

5.2.1. რესურსებით უზრუნველყოფა

ორგანიზაცია ვალდებულია განსაზღვროს და გამოყოს აუცილებელი რესურსები, რათა მოხდეს:

ა) იუმს ჩამოყალიბება, დანერგვა, ფუნქციონირება, მონიტორინგი, შენარჩუნება, განხილვა და გაუმჯობესება;

ბ) ინფორმაციული უსაფრთხოების პროცედურების მიერ ბიზნეს მოთხოვნების მხარდაჭერა;

გ) საკანონმდებლო და მარეგულირებელი მოთხოვნების და სახელშეკრულებო ვალდებულებების გამოვლენა და დაკმაყოფილება;

დ) ყველა დანერგილი კონტროლის მექანიზმის სათანადო გამოყენებით ადექვატური უსაფრთხოების შენარჩუნება;

ე) საჭიროების შემთხვევაში განხილვა და განხილვის შედეგად შესაბამისი რეაგირება;

ვ) იუმს-ის ეფექტიანობის გაუმჯობესება, სადაც ეს მიზანშეწონილი იქნება.

5.2.2. სწავლება, ინფორმირება და ცნობიერების ამაღლება

ორგანიზაციამ უდა უზრუნველყოს იუმს-ისთან მიმართებაში პერსონალის კვალიფიციურობა შემდეგი საქმიანობის შესრულებით:

ა) განისაზღვროს იუმს-ში ჩართული პერსონალის აუცილებელი ცოდნა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. მცოდნე პერსონალის აყვანა) საჭიროებების დასაკმაყოფილებლად;

გ) განხორციელებული ქმედებების ეფექტიანობის შეფასება;

დ) სწავლების, ტრენინგის, ცოდნის, გამოცდილების და კვალიფიკაციის შესახებ ინფორმაციის დაგროვება;

ორგანიზაციამ აგრეთვე უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელობას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

6. იუმს-ის შიდა აუდიტები

ორგანიზაცია ვალდებულია ჩაატაროს იუმს აუდიტი დაგეგმილ დროის ინტერვალებში და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები:

ა) შეესაბამება სტანდარტის, საკანონმდებლო და მარეგულირებელ მოთხოვნებს;

ბ) შეესაბამება გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება მისი დანერგვა და შენარჩუნება;

დ) მოქმედებს დაგეგმილის შესაბამისად.

აუდიტის პროგრამა უნდა დაიგეგმოს პროცესების და არეების მნიშვნელობის და სტატუსის გათვალისწინებით, აგრეთვე წინა აუდიტის შედეგების გათვალისწინებით. უნდა განისაზღვროს აუდიტის კრიტერიუმები, გავრცელების სფერო, სიხშირე და მიდგომა. აუდიტორების შერჩევამ და აუდიტის წარმოებამ უნდა უზრუნველყოს აუდიტის პროცესის ობიექტურობა და დამოუკიდებლობა. აუდიტორებმა არ უნდა შეამოწმონ საკუთარი ნამუშევარი. აუდიტის დაგეგვის და წარმოების უფლება-მოვალეობები და მოთხოვნები, აგრეთვე ანგარიშგების შედეგები უნდა განისაზღვროს დოკუმენტირებული პროცედურის მიერ (იხ. 4.3.3). მენეჯმენტს, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და გამომწვევი მიზეზების დაუყოვნებლივი აღმოფხვრა. გამოსწორების შემდეგ უნდა მოხდეს მისი შემოწმება და შემოწმების შედეგების შესახებ ანგარიშგება (იხ. 8).

შენიშვნა: ISO 19011:2002, Guidelines for quality and/or environmental management systems auditingწარმოადგენს სასარგებლო სახელმძღვანელოს იუმს-ის შიდა აუდიტის წარმოებისათვის.

7. იუმს-ის მენეჯერული განხილვა

7.1. ზოგადი

მენეჯმენტი ვალდებულია აწარმოოს იუმს-ის განხილვა დაგეგმილ დროის ინტერვალებში (სულ ცოტა წელიწადში ერთხელ) მიმდინარე შესაბამისობის, ადექვატურობისა და ეფექტიანობის უზრუნველსაყოფად. განხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვილებების

აუცილებლობას, ინფორმაციული უსაფრთხოების პოლიტიკისა და მიზნების გათვალისწინებით. განხილვის შედეგები ცალსახად უნდა იყოს დოკუმენტირებული და ჩანაწერები უნდა შენარჩუნდეს (იხ 4.3.3).

7.2. განსახილველი საკითხების ჩამონათვალი

მენეჯერული განხილვისთვის საჭირო საკითხები უნდა მოიცავდეს:

ა) იუმს-ის აუდიტის შედეგებს და განხილვებს;

ბ) დაინტერესებულ პირთა უკუკავშირს;

გ) იუმს წარმადობისა და ეფექტიანობის გაუმჯობესების ტექნიკას, პროდუქტს ან პროცედურას;

დ) პრევენციული ან მაკორექტირებელი ქმედებების სტატუსს;

ე) რისკების წინა შეფასების დროს არასათანადოდ რეაგირებულ სისუსტეებს ან საფრთხეებს;

ვ) ეფექტიანობის გაზომვის შედეგებს;

ზ) წინა სამენეჯერო განხილვის შემდგომ განხორციელებულ ქმედებებს;

თ) ნებისმიერ ცვლილებას, რომელმაც შესაძლოა გავლენა იქონიოს იუმს-ზე;

ი) გაუმჯობესების რეკომედაციებს.

7.3. განხილვის შედეგი

მენეჯერული განხილვის შედეგი უნდა მოიცავდეს ნებისმიერ გადაწყვეტილებას და ქმედებას შემდეგ საკითხებთან მიმართებაში:

ა) იუმს-ის ეფექტიანობის გაუმჯობესებას;

ბ) რისკების შეფასების და რისკების მოპყრობის გეგმის განახლებას;

გ) ინფორმაციული უსაფრთხოების პროცედურების და კონტროლის მექანიზმის ცვლილებას, რომელიც იუმს-ის შიდა ან გარე ფაქტორებისგან დაცვას ემსახურება, მათ შორის:

1. ბიზნეს მოთხოვნები;
2. უსაფრთხოების მოთხოვნები;
3. არსებულ ბიზნეს მოთხოვნებთან დაკავშირებული ბიზნეს-პროცესები;
4. მარეგულირებელი ან საკანონმდებლო მოთხოვნები;
5. საკონტრაქტო ვალდებულებები;
6. რისკის დონეები ან/და რისკის მიღების კრიტერიუმები;

დ) საჭირო რესურსები;

ე) კონტროლის მექანიზმების ეფექტიანობის შეფასების გაუმჯობესება.

8. იუმს-ის გაუმჯობესება

8.1.უწყვეტი გაუმჯობესება

ორგანიზაცია ვალდებულია მუდმივად გააუმჯობესოს იუმს-ის ეფექტიანობა ინფორმაციული უსაფრთხოების პოლიტიკის, ინფორმაციული უსაფრთხოების მიზნების, აუდიტის შედეგების, მონიტორინგის შედეგად აღმოჩენილი მოვლენების

ანალიზის, მაკორექტირებელი და პრევენციული ქმედებების და მენეჯერული განხილვის გზით (იხ. 7).

8.2. მაკორექტირებელი ქმედება

ორგანიზაცია ვალდებულია იუმს-ის მოთხოვნებთან შეუსაბამობების შემთხვევაში განახორციელოს გარკვეული ქმედება, რათა თავიდან აიცილოს ფაქტის განმეორება. მაკორექტირებელი ქმედების დოკუმენტირებული პროცედურა უნდა განსაზღვრავდეს:

ა) შეუსაბამობების აღმოჩენას;

ბ) შეუსაბამობების მიზეზების გამოვლენას;

გ) შეაფასოს ქმედების საჭიროება, რათა არ მოხდეს შეუსაბამობის განმეორება;

დ) გამოავლინოს და დანერგოს მაკორექტირებელი ქმედება;

ე) განხორციელებული ქმედების შედეგების დაფიქსირებას (იხ. 4.3.3);

ვ) მაკორექტირებელი ქმედების განხილვას.

8.3.პრევენციული ქმედება

ორგანიზაციამ უნდა განსაზღვროს იუმს-ის მოთხოვნებთან პოტენციური შეუსაბამობის აღმოსაფხვრელად საჭირო ქმედება, რათა თავიდან აიცილოს მათი დადგომა ან განმეორება. პრევენციული ქმედება პოტენციური პრობლემის შესაბამისი უნდა იყოს. პრევენციული ქმედების შესაბამისი დოკუმენტირებული პროცედურა უნდა განსაზღვრავდეს მოთხოვნებს შემდეგი საკითხებისთვის:

ა) პოტენციური შეუსაბამობის აღმოჩენა და მათ მიზეზები;

ბ) ქმედების საჭიროების შეფასება შეუსაბამობის თავიდან ასაცილებლად;

გ) პრევენციული ქმედების გამოვლენა და დანერგვა;

დ) განხორციელებული ქმედების შედეგის შესახებ ჩაწერის გაკეთება (იხ. 4.3.3);

ე) გატარებული პრევენციული ღონისძიების განხილვა.

ორგანიზაცია ვალდებულია გამოავლინოს შეცვლილი რისკები და პრევენციული ქმედებების მოთხოვნები, მნიშვნელოვანწილად შეცვლილ რისკებზე ყურადღების გამახვილებით. პრევენციული ქმედებების პრიორიტეტულობა უნდა განისაზღვრებოდეს რისკების შეფასების საფუძველზე.

შენიშვნა: ხშირად პრევენციული ქმედება უფრო ეფექტიანია ხარჯების მხრივ, ვიდრე მაკორექტირებელი ქმედება.

დანართი ა

ნორმატიული

კონტროლის მიზნები და კონტროლის მექანიზმები

ა.1 ცხრილში ჩამოთვლილი კონტროლის მიზნები და კონტროლის მექანიზმები პირდაპირ გამომდინარეობს და დაკავშირებულია მგს 27002:2011

სტანდარტის 5-დან 15-მდე პუნქტებთან. ცხრილის ჩამონათვალი არ არის სრულყოფილი და ორგანიზაციამ შესაძლოა ჩათვალოს, რომ საჭირო არის დამატებითი კონტროლების მიზნები და კონტროლის მექანიზმები. კონტროლის მიზნები და კონტროლის მექანიზმები ამ ცხრილიდან უნდა შეირჩეს როგორც 4.2.1-ში აღწერილი იუმს-ის პროცესის ნაწილი. მგს 27002:2011 სტანდარტის პუნქტები 5-დან 15-მდე წარმოადგენს დანერგვის სახელმძღვანელოს საუკეთესო პრაქტიკებიდან.

ცხრილი ა.1 - კონტროლის მიზნები და კონტროლის მექანიზმები

ა.5 უსაფრთხოების პოლიტიკა		
ა.5.1 ინფორმაციული უსაფრთხოების პოლიტიკა მიზანი: მოხდეს მენეჯმენტის მიმართვა და მხარდაჭერა ინფორმაციული უსაფრთხოების საკითხში ბიზნესის და საკანონმდებლო და მარეგულირებელ მოთხოვნებთან შესაბამისად.		
ა 5.1.1	ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტი	კონტროლის მექანიზმი: ინფორმაციული პოლიტიკა უნდა იყოს დამტკიცებული მენეჯმენტის მიერ და უნდა გამოქვეყნდეს და მიეწოდოს ყველა თანამშრომელს და გარე დაინტერესებულ მხარეს.
ა 5.1.2	ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა	კონტროლის მექანიზმი: ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა უნდა ხდებოდეს წინასწარ განსაზღვრულ დროის ინტერვალებში ან მნიშვნელოვანი ცვლილებების შემთხვევაში, რათა უზრუნველყოფილი იყოს მისი ვარგისიანობა, ადეკვატურობა და ეფექტიანობა.
ა.6 ინფორმაციული უსაფრთხოების ორგანიზება		
ა.6.1 შიდა ორგანიზება მიზანი: ორგანიზაციაში ინფორმაციული უსართხოების მართვა		
ა 6.1.1	ინფორმაციული უსაფრთხოებისადმი მენეჯმენტის მზადყოფნა	კონტროლის მექანიზმი: მენეჯმენტი ვალდებულია ორგანიზაციაში აქტიურად დაუჭიროს მხარი უსაფრთხოებას.
ა 6.1.2	ინფორმაციული უსაფრთხოების კოორდინირება	კონტროლის მექანიზმი: ინფორმაციული უსაფრთხოების საქმიანობები კოორდინირებული უნდა იყოს ორგანიზაციის სხვადასხვა ქვედანაყოფში შესაბამისი როლების და სამუშაოს გათვალისწინებით.
ა 6.1.3	ინფორმაციული უსაფრთხოების პასუხისმგებლობების განაწილება	კონტროლის მექანიზმი: ინფორმაციული უსაფრთხოების პასუხისმგებლობები ცალსახად უნდა იყოს განსაზღვრული.
ა 6.1.4	ინფორმაციის დამუშავების საშუალებათა ავტორიზაციის პროცესი	კონტროლის მექანიზმი: ყოველი ახალი ინფორმაციის დამუშავების საშუალებისადმი ავტორიზაცია უნდა იყოს განსაზღვრული და დანერგილი მენეჯმენტის

		მიერ.
ა 6.1.5	შეთანხმებები კონფიდენციალურობის შესახებ	კონტროლის მექანიზმი: ორგანიზაციაში ინფორმაციული უსაფრთხოების ამსახავი შეთანხმებები კონფიდენციალურობის და გაუმჟღავნებლობის შესახებ უნდა განისაზღვროს და პერიოდულად გადაიხედოს.
ა 6.1.6	კავშირი ხელისუფლებასთან	კონტროლის მექანიზმი: უნდა დამყარდეს ფორმალიზებული კავშირი შესაბამის მარეგულირებელ სახელმწიფო ინსტიტუტებთან
ა 6.1.7	კავშირი სპეციალურ დაინტერესებულ ჯგუფებთან	კონტროლის მექანიზმი: მოხდეს სპეციალურ დაინტერესებულ ჯგუფებთან და სპეციალისტთა უსაფრთხოების ფორუმებთან და პროფესიულ ასოციაციებთან ურთიერთობის შენარჩუნება.
ა 6.1.8	ინფორმაციული უსაფრთხოების დამოუკიდებელი განხილვა.	კონტროლის მექანიზმი: ინფორმაციული უსაფრთხოების მართვისადმი ორგანიზაციული მიდგომა და მისი დანერგვა (მაგ. ინფორმაციული უსაფრთხოების კონტროლის მიზნები, კონტროლის მექანიზმები, პოლიტიკები, პროცესები და პროცედურები) უდნა გადაიხედოს დამოუკიდებლად წინასწარ დაგეგმილ დროის ინტერვალებში, ან როდესაც მოხდება უსაფრთხოებაში მნიშვნელოვანი ცვლილება.
ა.6.2 მესამე მხარეები მიზანი: ორგანიზაციის ინფორმაციისა და მისი დამუშავების საშუალებების უსაფრთხოების შენარჩუნება, როდესაც მათზე წვდომა მესამე მხარის მიერ ხორციელდება		
ა 6.2.1	მესამე მხარეებთან დაკავშირებული რისკების აღმოჩენა	კონტროლის მექანიზმი: ორგანიზაციის და მესამე მხარის მიერ წვდომად, დამუშავებულ, მიწოდებულ და მართვად ინფორმაციასთან დაკავშირებული რისკები უნდა იქნეს გამოვლენილი და დაინერგოს შესაბამისი კონტროლის მექანიზმები, წვდომის უფლების მინიჭებამდე.
ა 6.2.2	კლიენტებთან ურთიერთობისას უსაფრთხოების ზომების მიღება	კონტროლის მექანიზმი: უსაფრთხოების მოთხოვნების შესაბამისი ყველანაირი ზომა უნდა იქნეს მიღებული, კლიენტების მხრიდან ორგანიზაციის ინფორმაციაზე ან აქტივებზე წვდომამდე.
ა 6.2.3	მესამე მხარეებთან შეთანხმებების დროს უსაფრთხოების ზომების მიღება	კონტროლის მექანიზმი: მესამე მხარეებთან შეთანხმებამ უნდა მოიცვას უსაფრთხოების ყველა შესაბამისი საკითხი, როდესაც ხდება მესამე მხარის მიერ ინფორმაციის დამუშავების საშუალებების ან ინფორმაციის წვდომა, დამუშავება, მასთან დაკავშირება ან მართვა.

ა.7 აქტივების მართვა		
ა.7.1 პასუხისმგებლობა აქტივებზე მიზანი: ორგანიზაციული აქტივების სათანადოდ დაცვა და შენარჩუნება		
ა 7.1.1	აქტივების ინვენტარიზაცია	კონტროლის მექანიზმი: ყველა აქტივი უნდა აღიწეროს და მოხდეს მნიშვნელოვანი აქტივების ინვენტარიზაცია
ა 7.1.2	აქტივების მფლობელობა	კონტროლის მექანიზმი: ყველა ინფორმაცია და ინფორმაციის დამუშავების საშუალებებთან დაკავშირებული ყველა აქტივი უნდა იყოს ორგანიზაციის გარკვეული ერთეულის მფლობელობაში
ა 7.1.3	აქტივების სათანადო გამოყენება	კონტროლის მექანიზმი: ინფორმაციის და ინფორმაციის დამუშავებასთან დაკავშირებული აქტივების დასაშვები მართვის წესები უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და დანერგვა.
ა.7.2 ინფორმაციის კლასიფიცირება მიზანი: ინფორმაციის სათანადო დაცვის დონის უზრუნველყოფა		
ა 7.2.1	კლასიფიკაციის სახელმძღვანელო	კონტროლის მექანიზმი: ინფორმაციის კლასიფიკაცია უნდა მოხდეს მისი ორგანიზაციაში ღირებულების, საკანონმდებლო მოთხოვნების, მგრძნობიარობისა და კრიტიკულობის გათვალისწინებით.
ა 7.2.2	ინფორმაციის მარკირება და მისი მოპყრობა	კონტროლის მექანიზმი: ჩამოყალიბდეს და დაინერგოს ინფორმაციის მარკირებისა და მისი მოპყრობის სათანადო პროცედურები ორგანიზაციაში მიღებული კლასიფიკაციის სქემის შესაბამისად.
ა.8 ადამიანური რესურსების უსაფრთხოება		
ა.8.1 დასაქმებამდე მიზანი: მომუშავე პერსონალის, კონტრაქტორების და მესამე მხარეების მიერ პასუხისმგებლობის გაცნობიერება, რათა მოხდეს დამუშავების საშუალებათა ქურდობის, თაღლითობის ან არამიზნობრივად გამოყენების თავიდან აცილება.		
ა 8.1.1	როლები და პასუხისმგებლობა	კონტროლის მექანიზმი: თანამშრომელთა, კონტრაქტორთა და მესამე მხარეთა როლები და პასუხისმგებლობა უნდა იყოს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისად განსაზღვრული და დოკუმენტირებული.
ა 8.1.2	გადამოწმება	კონტროლის მექანიზმი: უნდა განხორციელდეს დასაქმების კანდიდატების, კონტრაქტორების ან მესამე მხარეების შემოწმება კანონის, მარეგულირებლის და ეთიკის, ბიზნესის მოთხოვნების, სავარაუდო წვდომადი ინფორმაციის კლასიფიკაციის და სავარაუდო რისკების შესაბამისად,
ა 8.1.3	დასაქმების პირობები	კონტროლის მექანიზმი: დასაქმებულები, კონტრაქტორები და მესამე

		მხარეები ვალდებულნი არიან დაეთანხმონ და ხელი მოაწერონ დასაქმების კონტრაქტს, რომლის ფარგლებშიც იქნება განსაზღვრული მათი პასუხისმგებლობა ინფორმაციულ უსაფრთხოებაზე.
ა.8.2 დასაქმების პერიოდში მიზანი: დასაქმებულის, კონტრაქტორისა და მესამე მხარის შეტყობინება ინფორმაციული უსაფრთხოების საფრთხეების, მათი მოვალეობების და ვალდებულებების შესახებ, მათი უზრუნველყოფა აპარატურით, რათა მოხდეს ორგანიზაციული უსაფრთხოების პოლიტიკის მხარდაჭერა საქმიანობის დროს და შემცირდეს ადამიანური შეცდომის რისკი		
ა 8.2.1	მენეჯმენტის პასუხისმგებლობა	კონტროლის მექანიზმი: მენეჯმენტმა უნდა მოსთხოვოს თანამშრომლებს, კონტრაქტორებს და მესამე მხარეებს გამოიყენონ უსაფრთხოების ზომები ორგანიზაციაში არსებული უსაფრთხოების პოლიტიკების და პროცედურების შესაბამისად.
ა 8.2.2	ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლება, სწავლება და ტრენინგი	კონტროლის მექანიზმი: ორგანიზაციის ყველა თანამშრომელმა, და საჭიროების შემთხვევაში, კონტრაქტორებმა და მესამე მხარეებმა უნდა მიიღონ სათანადო ცნობიერების ამაღლების შესახებ ტრენინგი და ინფორმირებული იყვნენ ორგანიზაციული პოლიტიკების და პროცედურების განახლებების შესახებ, საქმიანობის შესრულების შესაბამისად.
ა 8.2.3	დისციპლინა	კონტროლის მექანიზმი: უნდა არსებობდეს გარკვეული დისციპლინარული პროცესი იმ თანამშრომლებისთვის, რომლებმაც საფრთხე შეუქმნეს ორგანიზაციის უსაფრთხოებას.
ა.8.3 სამსახურის შეცვლა ან გათავისუფლება მიზანი: თანამშრომლების, კონტრაქტორების და მესამე მხარეების ორგანიზაციიდან გასვლის, ან სამსახურებრივი პოზიციის შეცვლის წესების შესრულება		
ა 8.3.1	უფლებამოსილების შეწყვეტა	კონტროლის მექანიზმი: დასაქმების შეწყვეტის ან პოზიციის ცვლილების პასუხისმგებლობები უნდა იყოს ცალსახად განსაზღვრული და განაწილებული
ა 8.3.2	აქტივების დაბრუნება	კონტროლის მექანიზმი: ყველა დასაქმებული, კონტრაქტორი და მესამე მხარე დასაქმების შეწყვეტის შედეგად ვალდებულია დააბრუნოს მათ დაქვემდებარებაში არსებული ორგანიზაციის ყველა აქტივი.
ა 8.3.3	წვდომის უფლებების გაუქმება	კონტროლის მექანიზმი: თანამშრომელთა, კონტრაქტორთა და მესამე მხარეთა ინფორმაციაზე და ინფორმაციის დამუშავების საშუალებებზე წვდომის უფლებები უნდა გაუქმდეს საქმიანობის, კონტრაქტის ან შეთანხმების დასრულებასთან ერთად.

ა.9 ფიზიკური და გარემოს უსაფრთხოება		
ა.9.1 არეების დაცვა მიზანი: ორგაანიზაციის ინფორმაციაზე უნებართვო ფიზიკური წვდომის ან დაზიანების თავიდან აცილება.		
ა 9.1.1	ფიზიკური უსაფრთხოების პერიმეტრი	კონტროლის მექანიზმი: უსაფრთხოების პერიმეტრებში (ბარიერები, ისეთი როგორც კედლები, საბარათე კონტროლირებადი შესასვლელები, ან მისაღები ოთახები) ხდება ისეთი არეების დაცვა, სადაც განთავსებულია ინფორმაცია ან ინფორმაციის დამუშავების საშუალებები.
ა 9.1.2	ფიზიკური დაშვების კონტროლის მექანიზმები	კონტროლის მექანიზმი: დაცული არეების წვდომა უნდა იყოს შეზღუდული შესვლის კონტროლის შესაბამისი მექანიზმებით, რათა მხოლოდ ნებადართული პერსონალისთვის იყოს წვდომა შესაძლებელი.
ა 9.1.3	ოფისების, ოთახების და დამუშავების საშუალებების დაცვა	კონტროლის მექანიზმი: საჭიროა ოფისების, ოთახების და დამუშავების საშუალებების ფიზიკური დაცვის დაგეგმვა და გამოყენება.
ა 9.1.4	გარე და გარემოებრივი საფრთხეებისგან დაცვა	კონტროლის მექანიზმი: ხანძრის, დატბორვის, მიწისძვრის, აფეთქების, სამოქალაქო დაუმორჩილებლობის და სხვა ფორმის ბუნებრივი ან ადამიანური ფაქტორით გამოწვეული კატასტროფების საწინააღმდეგოდ უნდა დაიგეგმოს და დაინერგოს ფიზიკური უსაფრთხოება.
ა 9.1.5	დაცულ არეებში საქმიანობა	კონტროლის მექანიზმი: უდნა შეიქმნას და დაინერგოს ფიზიკური დაცვა და დაცულ არეებში მუშაობის სახელმძღვანელო მითითებები.
ა 9.1.6	საჯარო წვდომის, და მიღების/ჩატვირთვის არეები	კონტროლის მექანიზმები: საქონლის მიღების ან დაცლა/დატვირთვის არეებზე, სადაც შესაძლოა ადამიანების უნებართვო ყოფნა, უნდა განხორციელდეს კონტროლი, და თუ შესაძლებელია, ეს არეები იზოლირებული უნდა იყოს ინფორმაციის დამუშავების საშუალებებისგან, რათა არ მოხდეს მათზე უნებართვო წვდომა.
ა.9.2 მოწყობილობათა უსაფრთხოება მიზანი: ორგანიზაციის საქმიანობაში წყვეტის, აქტივების დაკარგვის, გაფუჭების ან მოპარვის თავიდან აცილება.		
ა 9.2.1	მოწყობილობათა განლაგება და დაცვა	კონტროლის მექანიზმი: მოწყობილობები განლაგებული ან დაცული უნდა იყოს გარემოს საფრთხეებისგან და უნებართვო წვდომისგან, რისკების შემცირების მიზნით.
ა 9.2.2	დამხმარე მოწყობილობები	კონტროლის მექანიზმი:

		დამუშავების საშუალებები დაცული უნდა იყოს ძაბვის ვარდნებისგან და სხვა გამანადგურებელი პროცესებისგან, რომელიც გამოწვეულია დამხმარე მოწყობილობებით.
ა 9.2.3	გაყვანილობის უსაფრთხოება	კონტროლის მექანიზმი: მონაცემთა დამუშავების დენის და საკომუნიკაციო გაყვანილობა უნდა იყოს დაცული ინფორმაციის მოპარვისა ან დაზიანებისგან.
ა 9.2.4	მოწყობილობათა მხარდაჭერა	კონტროლის მექანიზმი: უნდა მოხდეს მოწყობილობების მხარდაჭერა, რათა უზრუნველყოფილი იყოს მათი მუდმივი ხელმისაწვდომობა და სისრულე.
ა 9.2.5	ტერიტორიის გარეთ მყოფი მოწყობილობები	კონტროლის მექანიზმი: ტერიტორიის გარეთ მყოფ მოწყობილობებზე უნდა ვრცელდებოდეს დაცვა ტერიტორიის გარეთ საქმიანობის სხვადასხვა რისკის გათვალისწინებით.
ა 9.2.6	მოწყობილობათა უსაფრთხო განადგურება ან შემდგომი გამოყენება	კონტროლის მექანიზმი: განადგურებამდე ან ხელახლა გამოყენებამდე ყველა მოწყობილობის შემოწმება, არის თუ არა მასზე განთავსებული სენსიტიური ინფორმაცია და ლიცენზირებული პროგრამული უზრუნველყოფა წაშლილი.
ა 9.2.7	საკუთრების ამოღება	კონტროლის მექანიზმი: მოწყობილობები, ინფორმაცია ან პროგრამული უზრუნველყოფა არ უნდა გავიდეს ტერიტორიის გარეთ ნებართვის გარეშე.
ა.10 საკომუნიკაციო და საოპერაციო მართვა		
ა.10.1 საოპერაციო პროცედურები და პასუხისმგებლობები მიზანი: ინფორმაციის დამუშავების მოწყობილობების სწორი და უსაფრთხო მუშაობის უზრუნველყოფა		
ა 10.1.1	დოკუმენტირებული საოპერაციო პროცედურები	კონტროლის მექანიზმი: საოპერაციო პროცედურები უნდა იყოს დოკუმენტირებული და ხელმისაწვდომი ყველა მომხმარებლისთვის.
ა 10.1.2	ცვლილებათა მართვა	კონტროლის მექანიზმი: ინფორმაციის დამუშავების საშუალებების და სისტემების ცვლილებაზე უნდა ხორციელდებოდეს კონტროლი.
ა 10.1.3	მოვალეობათა განაწილება	კონტროლის მექანიზმი: მოვალეობები და პასუხისმგებლობის არეები უნდა იყოს გამიჯნული ორგანიზაციის აქტივების უნებართვო ან არაგანზრახ ცვლილების და ბოროტად გამოყენების თავიდან აცილების მიზნით.
ა 10.1.4	პროგრამული უზრუნველყოფის შემუშავების, სატესტო და საოპერაციო	კონტროლის მექანიზმი: პროგრამული უზრუნველყოფის შემუშავების,

	გარემოს გამიჯვნა	ტესტირების და საოპერაციო გარემო უნდა იყოს გამიჯნული უნებართვო წვდომის ან ცვლილებების რისკების შემცირების მიზნით.
ა.10.2 მესამე მხარის მიერ მოწოდებული მომსახურების მართვა მიზანი: შემუშავდეს და შენარჩუნდეს ინფორმაციული უსაფრთხოების და მომსახურების მოწოდების სათანადო დონეები მომსახურების მოწოდების შესახებ შეთანხმებების შესაბამისად.		
ა 10.2.1	მომსახურების მოწოდება	კონტროლის მექანიზმი: მომწოდებლის შეთანხმებაში არსებული უსაფრთხოების კონტროლის მექანიზმები უნდა დაინერგოს, მომსახურების ჩამონათვალი და მომსახურების მოწოდების დონეების მართვა უნდა ხდებოდეს მესამე მხარის მიერ.
ა 10.2.2	მესამე მხარის მიერ მოწოდებული მომსახურების მონიტორინგი და განხილვა.	კონტროლის მექანიზმი: უნდა ხდებოდეს მესამე მხარის მიერ მოწოდებული მომსახურების, ანგარიშების და ჩანაწერების რეგულარული მონიტორინგი და განხილვა, აგრეთვე მათი აუდიტი.
ა 10.2.3	მესამე მხარის მიერ მოწოდებული მომსახურების ცვლილების მართვა	კონტროლის მექანიზმი: მომსახურების მოწოდების ცვილება, მათ შორის არსებული ინფორმაციული უსაფრთხოების პოლიტიკის, პროცედურის ან კონტროლის მექანიზმის შენარჩუნება და გაუმჯობესება, უნდა იმართებოდეს ბიზნეს სისტემების კრიტიკულობის, გამოყენებული პროცესების და რისკების გადაფასების გათვალისწინებით.
ა.10.3 სისტემის დაგეგმვა და მიღება მიზანი: სისტემების ჩავარდნის რისკის შემცირება		
ა 10.3.1	სისტემის სიმძლავრეების მართვა	კონტროლის მექანიზმი: რესურსების გამოყენების მონიტორინგი, გაუმჯობესება და მომავალი სიმძლავრეებისადმი მოთხოვნების პროგნოზირება უნდა კეთდებოდეს სისტემის არსებითი ფუნქციების შესასრულებლად.
ა 10.3.2	სისტემის მიღება	კონტროლის მექანიზმი: ახალი საინფორმაციო სისტემის, სისტემის გაუმჯობესების და ახალი ვერსიების მიღების კრიტერიუმები უნდა ჩამოყალიბდეს, აგრეთვე უნდა ჩატარდეს სისტემის დამუშავების დროს და მის ჩაბარებამდე შესაბამისი ტესტირება.
ა.10.4 მავნე და მობილური კოდისგან დაცვა მიზანი: პროგრამული უზრუნველყოფის და ინფომაციის მთლიანობის დაცვა		
ა 10.4.1	მავნე კოდის საწინააღმდეგო კონტროლის მექანიზმები	კონტროლის მექანიზმი: მავნე კოდისგან დაცვის მიზნით საჭიროა დაინერგოს აღმოჩენის, პრევენციული და აღდგენის კონტროლის მექანიზმები, აგრეთვე მომხმარებლის ცნობიერების ამაღლების პროცედურები.

ა 10.4.2	მობილური კოდის საწინააღმდეგო კონტროლის მექანიზმები	კონტროლის მექანიზმი: იქ, სადაც მობილური კოდის გამოყენება ნებადართულია, კონფიგურაციამ უნდა უზრუნველყოს განსაზღვრულ პოლიტიკასთან მობილური კოდის ცალსახა შესაბამისობაში მუშაობა, და არაავტორიზებული კოდის მუშაობის აკრძალვა.
ა.10.5 სარეზერვო ასლები მიზანი: ინფორმაციის და ინფორმაციის დამუშავების მოწყობილობების მთლიანობის და ხელმისაწვდომობის მხარდაჭერა		
ა 10.5.1	ინფორმაციის სარეზერვო ასლები	კონტროლის მექანიზმი: ინფორმაციის და პროგრამული უზრუნველყოფის სარეზერვო ასლები პერიოდულად უნდა მოწმდებოდეს ორგანიზაციაში დანერგილი პოლიტიკის შესაბამისად.
ა.10.6 ქსელის უსაფრთხოების მართვა მიზანი: ქსელური ინფორმაციის და დამხმარე ინფრასტრუქტურის დაცვა		
ა 10.6.1	ქსელის კონტროლის მექანიზმები	კონტროლის მექანიზმი: ქსელის მართვა და კონტროლი უნდა ხორციელდებოდეს ადექვატურად, რათა უზრუნველყოფილი იყოს საფრთხეებისგან დაცვა ქსელში ჩართული სისტემებისა და პროგრამებისთვის, მათ შორის გადაცემის პროცესში მყოფი ინფორმაციისათვის.
ა 10.6.2	ქსელური მომსახურების უსაფრთხოება	კონტროლის მექანიზმი: ყველა ქსელური მომსახურების უსაფრთხოების ზომები, მომსახურების დონეები და მენეჯმენტის მოთხოვნები უნდა დადგინდეს და გათვალისწინებული იქნეს ქსელის მომსახურების შესახებ არსებულ შეთანხმებებში, მიუხედავად იმისა, ეს მომსახურება შიდაა თუ გარე.
ა.10.7 მედია-მატარებელების მართვა მიზანი: აქტივების უნებართვო გამჟღავნება, შეცვლა, ამოღება ან განადგურება, აგრეთვე ბიზნესის საქმიანობის შეწყვეტის თავიდან აცილება		
ა 10.7.1	გადაადგილებადი მედია-მატარებლების მართვა	კონტროლის მექანიზმი: უნდა ჩამოყალიბდეს გადაადგილებადი მედია-მატარებლების მართვის პროცედურები.
ა 10.7.2	მედია-მატარებლების განადგურება	კონტროლის მექანიზმი: ფორმალიზებული პროცედურის შესაბამისად უნდა მოხდეს მედია-მატარებლების უსაფრთხო განადგურება
ა 10.7.3	ინფორმაციის მოპყრობის პროცედურები	კონტროლის მექანიზმი: ინფორმაციის მოპყრობის და შენახვის პროცედურები უნდა ჩამოყალიბდეს, რათა ეს ინფორმაცია უნებართვო გამჟღავნებისგან ან გამოყენებისგან იყოს დაცული.

ა 10.7.4	სისტემის დოკუმენტაციის უსაფრთხოება	კონტროლის მექანიზმი: სისტემის დოკუმენტაცია უნდა იყოს დაცული არაავტორიზებული წვდომისაგან.
ა.10.8 ინფორმაციის გაცვლა მიზანი: ინფორმაციის და პროგრამული უზრუნველყოფის უსაფრთხოების შენარჩუნება ორგანიზაციის შიგნით ან სხვა გარე მხარესთან გაცვლისას.		
ა 10.8.1	ინფორმაციის გაცვლის პოლიტიკები და პროცედურები	კონტროლის მექანიზმი: ინფორმაციის უსაფრთხო გაცვლა ნებისმიერი საკომუნიკაციო საშუალებით უზრუნველყოფილი უნდა იყოს ფორმალური გაცვლის პოლიტიკებით, პროცედურებითა და კონტროლის მექანიზმებით.
ა 10.8.2	ინფორმაციის გაცვლის შესახებ შეთანხმებები	კონტროლის მექანიზმი: ინფორმაციის და პროგრამული უზრუნველყოფის გაცვლის შესახებ შეთანხმებები უნდა გაფორმდეს ორგანიზაციასა და გარე მხარეებს შორის.
ა 10.8.3	ფიზიკური მედია-მატარებლის გადაადგილება	კონტროლის მექანიზმი: ინფორმაციის მედია-მატარებელი უნდა იყოს დაცული არაავტორიზებული წვდომისაგან, გამოყენებისგან ან განადგურებისგან ორგანიზაციის ფარგლებს გარეთ გადაადგილების პროცესში.
ა 10.8.4	ელექტრონული მიმოწერა	კონტროლის მექანიზმი: ელექტრონულ მიმოწერაში მოხვედრილი ინფორმაცია უნდა იყოს სათანადოდ დაცული.
ა 10.8.5	ბიზნესის საინფორმაციო სისტემები	კონტროლის მექანიზმი: უნდა განისაზღვროს და დაინერგოს ბიზნესის საინფორმაცო სისტემების ურთიერთკავშირიდან გამომდინარე ინფორმაციის დაცვის პოლიტიკები და პროცედურები
ა.10.9 ელექტრონული კომერცია მიზანი: ელექტრონული კომერციის უსაფრთხოება და გამოყენება		
ა 10.9.1	ელექტრონული კომერცია	კონტროლის მექანიზმი: საჯარო ქსელებში მოძრავი ინფორმაცია ელექრტონული კომერციის შესახებ უნდა იყოს დაცული თაღლითობისგან, კონტრაქტის პირობების უგულებელყოფისგან და არაავტორიზებული გამჟღავნებისა და ცვლილებისგან.
ა 10.9.2	ონლაინ-ტრანზაქციები	კონტროლის მექანიზმი: ონლაინ-ტრანზაქციებში მონაწილე ინფორმაცია უნდა იყოს დაცული გადაგზავნის პროცესში წყვეტისგან, არასწორი გადაგზავნისგან, შეტყობინების არაავტორიზებული ცვლილებისგან, გამჟღავნებისგან, დუბლირებისგან ან ხელმეორედ გადაგზავნისაგან.

ა 10.9.3	საჯაროდ ხელმისაწმდომი ინფორმაცია	კონტროლის მექანიზმი: საჯაროდ ხელმისაწვდომი ან საჯარო სისტემაში არსებული ინფორმაციის მთლიანობა უნდა იყოს დაცული არაავტორიზებული ცვლილებისგან.
ა.10.10 მონიტორინგი მიზანი: ინფორმაციის არაავტორიზებული დამუშავების აღმოჩენა		
ა 10.10.1	აუდიტის შესახებ ჩანაწერები	კონტროლის მექანიზმი: მომხმარებლის მოქმედებები, გამონაკლისები, ინფორმაციის უსაფრთხოების მოვლენების შესახებ უნდა ხდებოდეს ჩანაწერების წარმოება და ინახებოდეს განსაზღვრული დროით, რათა დაეხმაროს მომავალ გამოძიებებში და წვდომის ზედამხედველობის კონტროლში.
ა 10.10.2	სისტემის გამოყენების მონიტორინგი	კონტროლის მექანიზმი: ინფორმაციის დამუშავების მოწყობილობების გამოყენების მონიტორინგის პროცედურები უნდა ჩამოყალიბდეს და მისი შედეგები გადაიხედოს პერიოდულად.
ა 10.10.3	ლოგირების ჩანაწერების დაცვა	კონტროლის მექანიზმი: ლოგირების მოწყობილობები და ლოგირების ჩანაწერები უდნა იყოს დაცული ცვლილებისგან და არაავტორიზებული წვდომისგან.
ა 10.10.4	ადმინისტრატორის და ოპერატორის ლოგები	კონტროლის მექანიზმი: უნდა ხდებოდეს სისტემის ადმინისტრატორის და სისტემის ოპერატორის მოქმედებათა ლოგირება.
ა 10.10.5	შეცდომების ლოგები	კონტროლის მექანიზმი: უნდა მოხდეს შეცდომების ლოგირება, მათი შესწავლა და განხორციელდეს შესაბამისი მოქმედება.
ა 10.10.6	საათის სინქრონიზაცია	კონტროლის მექანიზმი: ორგანიზაციის ან უსაფრთხოების ზონის ფარგლებში არსებული ინფორმაციული სისტემების საათი უნდა სინქრონიზირდებოდეს შეთანხმებულ სანდო დროის წყაროსთან.
ა.11 წვდომის კონტროლი		
ა.11.1 წვდომის კონტროლისთვის ბიზნეს მოთხოვნები მიზანი: ინფორმაციაზე წვდომის კონტროლი		
ა 11.1.1	წვდომის კონტროლის პოლიტიკა	კონტროლის მექანიზმი: წვდომის კონტროლის პოლიტიკა უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და გადაიხედოს ბიზნესის და უსაფრთხოების მოთხოვნებიდან გამომდინარე.
ა.11.2 მომხმარებელთა წვდომის მართვა მიზანი: ინფორმაციულ სისტემაში მომხმარებელთა ნებადართული წვდომის უზრუნველყოფა და არაავტორიზებული წვდომის თავიდან აცილება		
ა 11.2.1	მომხმარებელთა რეგისტრაცია	კონტროლის მექანიზმი:

		ინფორმაციულ სისტემაში მომხმარებლების დასაშვებად უნდა არსებობდეს ფორმალური რეგისტრაციისა და რეგისტრაცის გავლაზე უარის პროცედურა.
ა 11.2.2	პრივილეგიების მართვა	კონტროლის მექანიზმი: პრივილეგიების მინიჭება და მათი გამოყენება უნდა იყოს შეზღუდული და მართვადი.
ა 11.2.3	მომხმარებელთა პაროლების მართვა	კონტროლის მექანიზმი: პაროლების გაცემა უნდა იმართებოდეს მართვის ფორმალური პროცესის მიერ.
ა 11.2.4	მომხმარებელთა წვდომის უფლებების მიმოხილვა	კონტროლის მექანიზმი: მენეჯმენტმა პერიოდულად უნდა განიხილოს მომხმარბელთა წვდომის უფლებები.
ა.11.3 მომხმარებელთა პასუხისმგებლობები მიზანი: ინფორმაციაზე და ინფორმაციის დამუშავების მოწყობილობებზე არაავტორიზებული წვდომის, მათი უკანონო მითვისების და საფრთხის ქვეშ დაყენების თავიდან არიდება		
ა 11.3.1	პაროლების გამოყენება	კონტროლის მექანიზმი: მომხმარებელი ვალდებულია პაროლების შერჩევა და გამოყენება განახორციელოს არსებული საუკეთესო პრაქტიკების მიხედვით.
ა 11.3.2	უყურადღებოდ დატოვებული მოწყობილობები	კონტროლის მექანიზმი: მომხმარებლებმა უნდა უზრუნველყონ უმეთვალყურეოდ დარჩენილი მოწყობილობების სათანადოდდაცვა.
ა 11.3.3	„სუფთა მაგიდა და სუფთა ეკრანის“ პოლიტიკა	კონტროლის მექანიზმი: ნაბეჭდი მასალებისა და გადააადგილებადი მედია-მატარებლებისათვის უნდა გამოიყენებოდეს სუფთა მაგიდის პოლიტიკა, ინფორმაციის დამუშავების საშუალებებისათვის კი - სუფთა ეკრანის პოლიტიკა.
ა.11.4 ქსელური წვდომის კონტროლი მიზანი: ქსელურ სერვისებზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.4.1	ქსელური სერვისების გამოყენების პოლიტიკა	კონტროლის მექანიზმი: მომხმარებლებს უნდა მიეცეთ წვდომა მხოლოდ იმ რესურსებზე, რომლებზეც მათ გააჩნიათ ავტორიზებული უფლება.
ა 11.4.2	გარე კავშირისთვის მომხმარებელთა აუტენტიფიკაცია	კონტროლის მექანიზმი: სათანადო აუტენტიფიკაციის მეთოდები უნდა გამოიყენებოდეს დისტანციური მომხმარებლების მიერ წვდომის გასაკონტროლებლად.
ა 11.4.3	ქსელში არსებული მოწყობილობების იდენტიფიცირება	კონტროლის მექანიზმი: სხვადასხვა ადგილიდან ქსელური მოწყობილობების მიერთების აუტენტიფიკაციის მექანიზმი უნდა იყოს მოწყობილობათა ავტომატური იდენტიფიკაციის საშუალება.
ა 11.4.4	დაშორებული დიაგნოსტიკა და საკონფიგურაციო პორტების დაცვა	კონტროლის მექანიზმი: დიაგნოსტიკური და საკონფიგურაციო

		პორტების ფიზიკურ და ლოგიკურ წვდომაზე უნდა ხორციელდებოდეს კონტროლი.
ა 11.4.5	განცალკევება ქსელებში	კონტროლის მექანიზმი: ინფორმაციულ მომსახურებათა, მომხმარებელთა და საინფორმაციო სისტემათა ჯგუფები უნდა იყოს ქსელში განცალკევებული
ა 11.4.6	ქსელთან მიერთების კონტროლი	კონტროლის მექანიზმი: საერთო ქსელებისთვის, განსაკუთრებით რომლებიც ცდებიან ორგანიზაციის ფარგლებს, მომხმარებელთა ქსელთან მიერთების შესაძლებლობა უნდა იყოს შეზღუდული და იყოს წვდომის პოლიტიკის და ბიზნესის მხარდამჭერი სისტემების მოთხოვნებთან შესაბამისობაში.
ა 11.4.7	ქსელური მარშრუტიზაციის კონტროლი	კონტროლის მექანიზმი: ქსელების მარშრუტიზაციის კონტროლის მექანიზმები უნდა დაინერგოს ქსელებისთვის, რათა კომპიუტერის კავშირი და ინფორმაციის დინება დაცული იყოს გაჟონვისა და წვდომის პოლიტიკის დარღვევისგან.
ა.11.5 საოპერაციო სისტემაზე წვდომის კონტროლი მიზანი: საოპერაციო სისტემაზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.5.1	სისტემაში დაცული შესვლის პროცედურები	კონტროლის მექანიზმი: საოპერაციო სისტემებთან წვდომა უნდა ხდებოდეს შესვლის დაცული პროცედურის მიხედვით.
ა 11.5.2	მომხმარებელთა იდენტიფიკაცია და აუტენტიფიკაცია	კონტროლის მექანიზმი: ყველა მომხმარებელი უნდა ფლობდეს მხოლოდ მათი პერსონალური მოხმარებისთვის განკუთვნილ უნიკალურ იდენტიფიკატორს, და შესაბამისი აუტენტიფიკაციის მეთოდი უნდა იყოს არჩეული მომხმარებლის იდენტიფიკაციის საკმარისი მტკიცებულებისათვის.
ა 11.5.3	პაროლების მართვის სისტემა	კონტროლის მექანიზმი: პაროლების მართვის სისტემა უნდა იყოს ინტერაქტიული და უზრუნველყოფდეს ხარისხიან პაროლებს.
ა 11.5.4	დამხმარე სისტემური პროგრამების გამოყენება	კონტროლის მექანიზმი: სისტემის დამხმარე პროგრამების გამოყენება, რომლებსაც შეუძლიათ სისტემის შეზღუდვების და კონტროლების უგულებელყოფა, მკაცრად უნდა შეიზღუდოს და გაკონტროლდეს.
ა 11.5.5	სესიის ვადის ამოწურვა	კონტროლის მექანიზმი: არააქტიური სესიები უნდა დაიხუროს წინასწარ დადგენილი ვადის გასვლის შემდეგ.
ა 11.5.6	დაკავშირების ხანგრძლივობის შეზღუდვა	კონტროლის მექანიზმი: უნდა დადგინდეს დაკავშირების ხანგრძლივობის შეზღუდვა მაღალი რისკის

		შემცველი პროგრამული უზრუნველყოფის დამატებითი დაცვისათვის.
ა.11.6 პროგრამული უზრუნველყოფზე და ინფორმაციაზე წვდომის კონტროლი მიზანი: პროგრამულ უზრუნელყოფაში არსებულ ინფორმაციაზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.6.1	ინფორმაციაზე წვდომის შეზღუდვა	კონტროლის მექანიზმი: მომხმარებელთა და დამხმარე პერსონალის წვდომა ინფორმაციაზე და იფნორმაციული სისტემების ფუნქციებზე უნდა იყოს შეზღუდული წვდომის პოლიტიკის შესაბამისად.
ა 11.6.2	სენსიტიური ინფორმაციის იზოლირება	კონტროლის მექანიზმი: სენსიტიურ სისტემებს უნდა გააჩნდეთ გამოყოფილი (იზოლირებული) გარემო.
ა.11.7 მობილური ტექნოლოგიები და დისტანციური მუშაობა მიზანი: ინფორმაციის უსაფრთხოების უზრუნველყოფა მობილური ტექნოლოგიებისა და და დისტანციური მუშაობის შემთხვევაში.		
ა 11.7.1	მობილური ტექნოლოგიების გამოყენება და კავშირგაბმულობა	კონტროლის მექანიზმი: პოლიტიკა უნდა ჩამოყალიბდეს და შესაბამისი უსაფრთხოების ზომები უნდა იქნეს მიღებული მობილური ტექნოლოგიების და კავშირგაბმულობის გამოყენებისას რისკებისგან თავის დასაცავად.
ა 11.7.2	დისტანციური მუშაობა	კონტროლის მექანიზმი: პოლიტიკა, საოპერაციო გეგმა და პროცედურები უნდა შემუშავდეს და დაინერგოს დისტანციური მუშაობის შემთხვევაში.
ა.12 ინფორმაციული სისტემების შეძენა, დამუშავება და შენარჩუნება		
ა.12.1 ინფორმაციული სისტემების უსაფრთხოების მოთხოვნები მიზანი: უზრუნველყოფილი უნდა იყოს უსაფრთხოება, როგორც ინფორმაციული სისტემის განუყოფელი ნაწილი		
ა 12.1.1	უსაფრთხოების მოთხოვნების ანალიზი და მახასიათებლები	კონტროლის მექანიზმი: უსაფრთხოების კონტროლის მოთხოვნები უნდა იყოს ახალი სისტემის ან არსებული სისტემის გაუმჯობესებისთვის საჭირო ბიზნეს-მოთხოვნების ნაწილი
ა.12.2 პროგრამული უზრუნველყოფის სწორი დამუშავება მიზანი: პროგრამულ უზრუნველყოფაში არსებული ინფორმაციის შეცდომების, დაკარგვის, არაავტორიზებული ცვლილებისა და გამოყენებისგან დაცვა		
ა 12.2.1	შემავალი მონაცემების შემოწმება	კონტროლის მექანიზმი: პროგრამულ უზრუნველყოფაში შემავალი ინფორმაცია უნდა მოწმდებოდეს სისწორეზე და შესაბამისობაზე.
ა 12.2.2	შიდა დამუშავების კონტროლი	კონტროლის მექანიზმი: პროგრამულ უზრუნველყოფას უნდა გააჩნდეს შემოწმების საშუალებები, რათა აღმოჩენილ იქნეს ინფორმაციის ნებისმიერი დაზიანება დამუშავების პროცესში ან განზრახ ქმედების

		შედეგად.
ა 12.2.3	შეტყობინების მთლიანობა	კონტროლის მექანიზმი: პროგრამულ უზრუნველყოფაში უნდა დაინერგოს შეტყობინების აუტენტურობის და მთლიანობის დამცავი მოთხოვნები, ასევე გამოვლინდეს და დაინერგოს შესაბამისი კონტროლის მექანიზმები
ა 12.2.4	გამომავალი ინფორმაციის შემოწმება	კონტროლის მექანიზმი: პროგრამული უზრუნველყოფის გამომავალი ინფორმაცია უნდა მოწმდებოდეს არსებული ინფორმაციის დამუშავების სისწორეზე და შესაბამისობაზე.
ა.12.3 კრიფტოგრაფიული კონტროლის მექანიზმები მიზანი: ინფორმაციის კონფიდენციალურობის, აუტენტურობის და მთლიანობის დაცვა კრიპტოგრაფიული საშუალებებით.		
ა. 12.3.1	კრიპტოგრაფიული მეთოდების გამოყენების პოლიტიკა	კონტროლის მექანიზმი: ინფორმაციის დაცვის კრიპტოგრაფიული მეთოდების გამოყენების პოლიტიკა უნდა ჩამოყალიბდეს და დაინერგოს.
ა 12.3.2	გასაღებების მართვა	კონტროლის მექანიზმი: ორგანიზაციაში კრიპტოგრაფიული ხერხების გამოყენების მიზნით უნდა არსებობდეს გასაღებების მართვის პროცესი.
ა.12.4 სისტემური ფაილების უსაფრთხოება მიზანი: სისტემური ფაილების უსაფრთხოების უზრუნველყოფა		
ა 12.4.1	საოპერაციო სისტემების კონტროლი	კონტროლის მექანიზმი: საოპერაციო სისტემებზე პროგრამების ინსტალაცია უნდა კონტროლდებოდეს შესაბამისი პროცედურის მიერ.
ა 12 4.2	სისტემის სატესტო მონაცემების დაცვა	კონტროლის მექანიზმი: სატესტო მონაცემების შერჩევა უნდა მოხდეს ყურადღებით, იყოს დაცული და კონტროლდებოდეს.
ა 12.4.3	პროგრამის კოდზე წვდომის კონტროლი	კონტროლის მექანიზმი: პროგრამის კოდზე წვდომა უნდა იყოს შეზღუდული.
ა.12.5 უსაფრთხოება დამუშავებასა და მხარდამჭერ პროცესებში მიზანი: პროგრამული სისტემის და ინფორმაციის უსაფრთხოების შენარჩუნება		
ა 12.5.1	ცვლილების კონტროლის პროცედურები	კონტროლის მექანიზმი: ცვლილებების დანერგვა უნდა კონტროლდებოდეს ცვლილების კონტროლის პროცედურების მიხედვით.
ა 12.5.2	საოპერაციო სისტემის ცვლილებების შემდგომი პროგრამული უზრუნველყოფის ტექნიკური მიმოხილვა	კონტროლის მექანიზმი: იმ შემთხვევაში, როდესაც ხდება საოპერაციო სისტემის ცვლილება, უნდა მოხდეს ბიზნესის კრიტიკული პროგრამული უზრუნველყოფის განხილვა და ტესტირება ორგანიზაციის

		ოპერაციებზე და უსაფრთხოებაზე უარყოფითი გავლენის თავიდან ასაცილებლად.
ა 12.5.3	პროგრამული პაკეტების ცვლილებების შეზღუდვა	კონტროლის მექანიზმი: პროგრამული პაკეტების ცვლილებები უნდა განხორციელდეს მხოლოდ აუცილებელობის შემთხვევაში და უნდა კონტროლდებოდეს მკაცრად.
ა 12.5.4	ინფორმაციის გაჟონვა	კონტროლის მექანიზმი: ინფორმაციის შესაძლო გაჟონა უნდა იქნეს თავიდან არიდებული.
ა 12.5.5	პროგრამის შექმნა/დამუშავება მესამე მხარის მიერ.	კონტროლის მექანიზმი: უნდა ხდებოდეს მესამე მხარის მიერ შექმნილი/დამუშავებული პროგრამების ზედამხედველობა და ორგანიზაციის მიერ მათზე მონიტორინგის განხორციელება.
ა.12.6 ტექნიკური სისუტეების მართვა მიზანი: ცნობილი ტენიკური სისუსტეებით სარგებლობისგან გამოწვეული რისკის შემცირება		
ა 12.6.1	ტექნიკური სისუსტეების მართვა	კონტროლის მექანიზმი: ინფორმაციული სისტემების ტექნიკური სისუსტეების შესახებ მოძიებული უნდა იქნეს ოპერატიული ინფორმაცია, ორგანიზაციის ამ სისუსტეებისადმი დამოკიდებულება შეფასდეს, და შესაბამისი ზომები მიღებულ იქნეს არსებული რისკებზე რეაგირებისთვის.
ა.13 ინფორმაციული უსაფრთხოების ინციდენტების მართვა		
ა.13.1 ინფორმაციული უსაფრთხოების მოვლენების და სისუსტეების შესახებ ანგარიში მიზანი: ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მოვლენების და სისუსტეების შესახებ შეტყობინებები ხდება დროულად		
ა 13.1.1	ინფორმაციული უსაფრთხოების მოვლენების ანგარიში	კონტროლის მექანიზმი: ინფორმაციული უსაფრთხოების მოვლენების შესახებ ანგარიშგება ხდება ოპერატიულად შესაბამისი მართვის არხების მეშვეობით
ა 13.1.2	უსაფრთხოების სისუსტის ანგარიში	კონტროლის მექანიზმი: ინფორმაციული სისტემის და მომსახურების გამომყენებელი ყველა თანამშრომელი, კონტრაქტორი ან მესამე მხარის მომხმარებელი ვალდებულია აცნობოს შენიშნული ან სავარაუდო უსაფრთხოების სისუსტის შესახებ.
ა.13.2 ინფორმაციული უსაფრთხოების ინციდენტების და გაუჯობესებების მართვა მიზანი: უზრუნველყოფილი უნდა იყოს მუდმივი და ეფექტიანი მიდგომის გამოყენება ინფორმაციული უსაფრთხოების ინციდენტების მართვაში.		
ა 13.2.1	პასუხისმგებლობები და პროცედურები	კონტროლის მექანიზმი: უნდა განისაზღვროს მენეჯმენტის პასუხისმგებლობები და პროცედურები, რათა მოხდეს სწრაფი, ეფექტიანი და სათანადო რეაგირება ინფორმაციული უსაფრთხოების ინციდენტზე.

ა 13.2.2	ინფორმაციული უსაფრთხოების ინციდენტებიდან მიღებული ცოდნა	კონტროლის მექანიზმი: უნდა არსებობდეს მექანიზმი, რომლის მეშვეობითაც მოხდება ინფორმაციული უსაფრთხოების ინციდენტების აღრიცხვა და ზედამხედველობა მისი ტიპის, მოცულობის და ღირებულების მიხედვით.
ა 13.2.3	მტკიცებულებების მოძიება	კონტროლის მექანიზმი: უნდა მოხდეს მტკიცებულებების მოძიება, დაცვა და წარდგენა, როდესაც პიროვნების ან ორგანიზაციის წინააღმდეგ ხორციელდება სამოქალაქო ან სისხლის სამართლის წარმოება.
ა.14 ბიზნესის უწყვეტობის მართვა		
ა.14.1 ბიზნესის უწყვეტობის მართვის ინფორმაციული უსაფრთხოების ასპექტები. მიზანი: ბიზნესის წყვეტის წინააღმგედ და ბიზნესის კრიტიკული პროცესების დასაცავად მიმართული ქმედება, ინფორმაციული სისტემის მნიშვნელოვანი წარუმატებლობის/მარცხის ან სტიქიური უბედურების შემთხვევაში დროული აღდგენა.		
ა 14.1.1	ბიზნესის უწყვეტობის მართვის პროცესში ინფორმაციული უსაფრთხების გათვალისწინება.	კონტროლის მექანიზმი: უნდა შემუშავდეს და შენარჩუნდეს ორგანიზაციის ბიზნესის უწყვეტობის პროცესი, რომელიც ივალისწინებს ინფორმაციული უსაფრთხოების მოთხოვნებს.
ა 14.1.2	ბიზნესის უწყვეტობა და რისკების შეფასება	კონტროლის მექანიზმი: გამოვლენილი უნდა იყოს ის მოვლენები, რომლებმაც შესაძლოა იმოქმედოს ბიზნეს-პროცესების წყვეტაზე, აგრეთვე ამ წყვეტის ალბათობა, ეფექტი და გავლენა ინფორმაციულ უსაფრთხოებაზე.
ა 14.1.3	ინფორმაციული უსაფრთხოების შემცველი ბიზნესის უწყვეტობის გეგმების შემუშავება	კონტროლის მექანიზმი: უნდა შემუშავდეს და დაინერგოს გეგმები, რომლებიც მოიცავს ოპერაციების შენარჩუნებას ან აღდგენას, ასევე სათანადო დონეზე და მისაღებ დროში ბიზნეს პროცესის წყვეტის ან გაჩერების შემდეგ უზრუნველყოფს ინფორმაციის ხელმისაწვდომობას.
ა 14.1.4	ბიზნესის უწყვეტობის დაგეგმარების სტრატეგია.	კონტროლის მექანიზმი: უნდა შემუშავდეს ბიზნესის უწყვეტობის ერთიანი დაგეგმარების სტრატეგია ყველა გეგმის თავსებადობაში მოსაყვანად, რომელიც თანმიმდევრულად პასუხობს ინფორმაციული უსაფრთხოების მოთხოვნებს, აღწერს ტესტირების და შენარჩუნების პრიორიტეტებს.
ა 14.1.5	ბიზნეს უწყვეტობის გეგმების ტესტირება, შენარჩუნება და ხელახლა შეფასება	კონტროლის მექანიზმი: უნდა ხდებოდეს ბიზნეს უწყვეტობის გეგმების რეგულარული ტესტირება და განახლება მათი თანამედროვეობის და

		ეფექტიანობის უზრუნველსაყოფად.
ა.15 შესაბამისობა		
ა.15.1 იურიდიულ მოთხოვნებთან შესაბამისობა მიზანი: ნებისმიერი იურიდიული, მარეგულირებელი და საკონტრაქტო ვალდებულებების და უსაფრთხოების მოთხოვნების დარღვევის თავის არიდება.		
ა 15.1.1	გამოსაყენებელი იურიდიული ბაზის დადგენა	კონტროლის მექანიზმი: ყველა მნიშვნელოვანი იურიდიული, მარეგულირებელი და საკონტრაქტო მოთხოვნა და ორგანიზაციის მიდგომა ამ მოთხოვნების დაკმაყოფილებისადმი უნდა განისაზღვროს ცალსახად და იყოს მოქმედი ყოველი საინფორმაციო სისტემისა და ორგანიზაციისთვის.
ა 15.1.2	ინტელექტუალური საკუთრების უფლებები	კონტროლის მექანიზმი: ინტელექტუალური საკუთრების ან კერძო პროგრამული პროდუქტის გამოყენების შემთხვევაში უნდა დაინერგოს შესაბამისი პროცედურა, რომელიც უზრუნველყოფს იურიდიულ, მარეგულირებელ და საკონტრაქტო მოთხოვნებთან შესაბამისობას.
ა 15.1.3	ორგანიზაციული ჩანაწერების დაცვა	კონტროლის მექანიზმი: მნიშვნელოვანი ორგანიზაციული ჩანაწერები უნდა იყოს დაცული დაკარგვისგან, განადგურებისგან და გაყალბებისგან კანონის მიერ დადგენილ, მარეგულირებელ, საკონტრაქტო და ბიზნეს-მოთხოვნებთან შესაბამისად.
ა 15.1.4	მონაცემთა დაცვა და პირადი ინფორმაციის საიდუმლოება	კონტროლის მექანიზმი: მონაცემთა დაცვა და საიდუმლოება უნდა იყოს უზრუნველყოფილი იურიდიული, მარეგულირებელი და, როდესაც სჭიროა, საკონტრაქტო ვალდებულებების შესაბამისად.
ა 15.1.5	ინფორმაციის დამუშავების საშუალებათა არამიზნობრივად გამოყენების აღკვეთა	კონტროლის მექანიზმი: ინფრომაციის დამუშავების საშუალებების არამიზნობრივად გამოყენება მომხმარებლების მიერ უნდა აღიკვეთოს.
ა 15.1.6	კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენების რეგულაცია	კონტროლის მექანიზმი: კრიპტოგრაფიული კონტროლის მექანიზმები უნდა გამოყენებოდეს იურიდიული, მარეგულირებელი და საკონტრაქტო მოთხოვნების შესაბამისად.
ა.15.2 უსაფრთხოების პოლიტიკებთან და სტანდარტებთან შესაბამისობა და ტექნიკური შესაბამისობა მიზანი: სისტემების შესაბამისობის უზრუნველყოფა ორგანიზაციის უსაფრთხოების პოლიტიკებსა და სტანდარტებთან		

ა 15.2.1	უსაფრთხოების პოლიტიკებსა და სტანდარტებთან შესაბამისობა.	კონტროლის მექანიზმი: მენეჯერებმა უნდა უზრუნველყონ საკუთარი პასუხისმგებლობის არეში მოქმედი ყველა უსაფრთხოების პროცედურის შესრულება უსაფრთხოების პოლიტიკებსა და სტანდარტებთან შესაბამისობის მისაღწევად.
ა 15.2.2	ტექნიკური შესაბამისობის შემოწმება	კონტროლის მექანიზმი: ინფორმაციული სისტემები მუდმივად უნდა მოწმდებოდეს უსაფრთხოების დანერგვის სტანდარტებთან შესაბამისობაზე.
ა.15.3 ინფორმაციული სისტემების აუდიტის რეკომენდაციები მიზანი: ინფორმაციული სისტემების აუდიტის პროცესის შედეგის ეფექტიანობის გაზრდა და მისი ჩარევის მინიმუმამდე დაყვანა.		
ა 15.3.1	ინფორმაციული სისტემების აუდიტის კონტროლები	კონტროლის მექანიზმი: საოპერაციო სისტემების აუდიტის მოთხოვნები და ქმედებები საგულდაგულოდ უნდა დაიგეგმოს და შეთანხმდეს ბიზნეს-პროცესის წყვეტის რისკის შესამცირებლად.
ა 15.3.2	ინფორმაციული სისტემების აუდიტის საშუალებების დაცვა.	კონტროლის მექანიზმი: ინფორმაციული სისტემების აუდიტის საშუალებების წვდომა უნდა იყოს დაცული არაავტორიზებული გამოყენებისა და კომპრომეტირებისგან.

მუხლი 3. გარდამავალი დებულება

1. საჯარო სამართლის იურიდიული პირი - კიბერუსაფრთხობის ბიურომ 2014 წლის 1 სექტემბრამდე შეიმუშაოს:

ა) თავდაცვის სფეროში კრიტიკული ინფორმაციული სუბიექტებისათვის აუცილებელი შესასრულებელი მოთხოვნები.

ბ) თავდაცვის სფეროში კრიტიკული ინფორმაციული ტექნოლოგიების უსაფრთხოების საშუალებების ინფორმაციული უსაფრთხოების მართვის სისტემები-მოთხოვნების შემუშავება.

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

თავი I ზოგადი დებულებები

მუხლი 1. შესავალი

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები (შემდგომში

- „მოთხოვნები“) შესასრულებლად სავალდებულოა კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის (შემდგომში - „ორგანიზაცია“).

2. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები“ თავსებადობაშია, ერთი მხრივ, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონთან, ხოლო, მეორეს მხრივ, ISO 27000 სერიის სტანდარტებთან.

მუხლი 2. ტერმინები და განმარტებები

1. ამ ბრძნებაში გამოყენებული ტერმინები და განმარტები არ უნდა განიმარტოს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით დადგენილი ანალოგიური ტერმინებისაგან გასხვავებულად, არამედ გამოიყენება როგორც კანონით დადგენილი ტერმინების დამატებითი და დამაზუსტებელი განმარტებები.

2. ბრძანებაში გამოყენებული ტერმინებს ამ ბრძნების მიზნებისთვის აქვს შემდეგი განმარტებები:

ა) ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები - საბაზისო მოთხოვნები, სავალდებულოა შესრულდეს თანმიმდევრულად სამი წლის ვადაში ინფორმაციული უსაფრთხოების მართვის სისტემის დასანერგად;

ბ) ინფორმაციული აქტივი (შემდგომში - „აქტივი“) – ყველა ინფორმაცია და ცოდნა (კერძოდ,

ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

გ) ავტორიზებული ერთეული - ინდივიდი, სუბიექტი ან პროცესი, რომელსაც გააჩნია აქტივზე წვდომის უფლება;

დ) ხელმისაწვდომობა - ავტორიზებული სუბიექტის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი;

ე) კონფიდენციალურობა - აქტივის მახასიათებელი, რომლის თანახმადაც აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის;

ვ) მთლიანობა - აქტივის სიზუსტის და სისრულის მახასიათებელი;

ზ) ინფორმაციული უსაფრთხოება - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, აუთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

თ) ინფორმაციული უსაფრთხოების მართვის სისტემა - იუმს - მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონერება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

ი) რეაგირების გარეშე დარჩენილი რისკი - რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

კ) რისკის მიღება - გადაწყვეტილება რისკის მიღების თაობაზე;

ლ) რისკის ანალიზი - ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მის მიერ მიყენებული შესაძლო ზიანის დასადგენად;

მ) რისკის დონის დადგენა - რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

ნ) რისკების მართვა - მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

ო) რისკების მოპყრობა - რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

პ) კონტროლის მექანიზმების გამოყენებადობის განაცხადი - იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

თავი II
ორგანიზაციისათვის პირველ წელს შესასრულებელი მოთხოვნები

მუხლი 3. ორგანიზაციაში ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ხელმძღვანელობის მხრიდან მხარდაჭერა

ორგანიზაციაში უნდა არსებობდეს შიდასამსახურებრივი დოკუმენტი ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის შესახებ (იხ. დანართი 1, მგს 27001:2011, თავი 5.1 და 5.2; აგრეთვე დანართი ა-დან კონტროლი ა.6.1.1.).

მუხლი 4. ორგანიზაციული მოწყობა

ორგანიზაციამ უნდა განსაზღვროს პირი ან პირები (მაგალითად, ინფორმაციული უსაფრთხოების საბჭო, რომელიც შედგება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისაგან), რომელიც განახორციელებს ინფორმაციული უსაფრთხოების მართვას (იხ. დანართი 1, მგს 27001:2011, თავი 5.1; კონტროლები: ა.6.1.1; ა.6.1.2; ა.6.1.3.“).

მუხლი 5. გავრცელების სფერო

ორგანიზაციამ უნდა განსაზღვროს და დოკუმენტირებულად წარმოადგინოს იუმს-ის გავრცელების სფერო და საზღვრები საქმიანობის, ორგანიზაციული სტრუქტურის, ადგილმდებარეობის, აქტივებისა და ტექნოლოგიების ჭრილში, მათ შორის დაასაბუთოს დაშვებული გამონაკლისების მიზეზები და შეათანხმოს ისინი საქართველოს თავდაცვის სამინისტროსთან (შემდგომში - „სამინისტრო“) (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ა).

მუხლი 6. იუმს-ის პოლიტიკა

1. ორგანიზაციამ უნდა წარმოადგინოს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) პოლიტიკის დოკუმენტი, რომელშიც ასახული იქნება ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების მართვის სისტემის ხედვა, დასახული მიზნები და სასურველი შედეგები და დამტკიცებული იქნება ხელმძღვანელობის მიერ (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-5).

2. ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემა უნდა უზრუნველყოფდეს დაგეგმვის, დანერგვის, ფუნქციონირების, მონიტორინგისა და გაუმჯობესებისთვის საჭირო ფაზებს (იხ. დანართი 1, მგს 27001:2011, თავები: 4.1; 4.3.1ა,ბ,გ; კონტროლები: ა.5.1.1; ა.5.1.2“).

3. ინფორმაციული უსაფრთხოების პოლიტიკა:

ა) შეიცავს ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანს, ძირითად მიმართულებას და პრინციპებს (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-1);

ბ) ითვალისწინებს განაცხადს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის და სხვა სტანდარტების მოთხოვნებთან შესაბამისობის შესახებ (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-2; კონტროლი ა. 15.1);

გ) პასუხობს ორგანიზაციის რისკების მართვის კონტექსტს, რომლის ფარგლებშიც მოხდება იუმს-ის ჩამოყალიბება და მხარდაჭერა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ბ-3).

მუხლი 7. აქტივების გამოვლენა, აღწერა, კლასიფიცირება და მართვა,

1. ორგანიზაციამ უნდა განახორციელოს დადგენილ გავრცელების სფეროში აქტივების მართვა, რაც გულისხმობს აქტივების გამოვლენის, აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და უზრუნველყოფას. (ასევე, იხ. დანართი 1, მგს 27001:2011, კონტროლები: ა.7.1 და ა.7.2 სრულად).

2. ორგანიზაციამ აქტივების მართვა უნდა განახორციელოს „ინფორმაციული აქტივების მართვის წესების შესახებ“ საქართველოს თავდაცვის მინისტრის ბრძანების შესაბამისად.

მუხლი 8. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

1. ორგანიზაციამ უნდა შეიმუშავოს და განახორციელოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ე). ორგანიზაციამ უნდა უზრუნველყოს პერსონალის კვალიფიციურობა იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

ა) იუმს-ში ჩართული პერსონალისთვის აუცილებელი ცოდნის განსაზღვრა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

გ) სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ ჩანაწერების წარმოება.

2. ორგანიზაციამ უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

თავი III
ორგანიზაციისათვის მეორე წელს შესასრულებელი მოთხოვნები

მუხლი 9. რისკების მოპყრობის გეგმა

1. ორგანიზაციამ უნდა ჩამოაყალიბოს და დანერგოს რისკების მოპყრობის გეგმა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ა-ბ), რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო ქმედებებს ხელმძღვანელობის მხრიდან, რესურსებს (იხ. დანართი 1, მგს 27001:2011, თავი 5.2.1), პასუხისმგებლობებს და პრიორიტეტებს.

2. ორგანიზაციამ უნდა უზრუნველყოს კონტროლის მიზნების მიღწევა, რაც გულისხმობს სახსრების განაწილებას და პასუხისმგებლობების და როლების განსაზღვრას.

მუხლი 10. ორგანიზაციაში კონტროლის მექანიზმების დანერგვა

ინფორმაციული უსაფრთხოების მიზნების მისაღწევად ორგანიზაციამ უნდა:

ა) დანერგოს მეორე წლის მე-14 მუხლის მე-5 პუნქტში შერჩეული კონტროლის მექანიზმები;

ბ) კონტროლის მექანიზმების დანერგვისთანავე ორგანიზაციამ უნდა აწარმოოს მათზე დაკვირვება;

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

მუხლი 11. კონტროლის მექანიზმების ეფექტიანობის საზომების განსაზღვრა

1. ორგანიზაციამ უნდა განსაზღვროს შერჩეული კონტროლის მექანიზმების ან კონტროლის მექანიზმთა ჯგუფის ეფექტიანობის საზომები და დაადგინოს თუ როგორ და ვის მიერ მოხდება ამ საზომების გამოყენება, რათა შეფასდეს კონტროლის მექანიზმების ეფექტიანობა და მიღებული იქნას შედარებადი და განმეორებადი შედეგები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.დ).

2. კონტროლის მექანიზმის ეფექტიანობის გაზომვა ხელმძღვანელობას და პერსონალს საშუალებას აძლევს განსაზღვრონ, შერჩეული კონტროლის მექანიზმი რამდენად ეფექტიანად იძლევა კონტროლის მიზნების მიღწევის საშუალებას.

მუხლი 12. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

1. ორგანიზაციამ უნდა შეიმუშავოს და განახორციელოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.2.ე). ორგანიზაციამ უნდა უზრუნველყოს პერსონალის კვალიფიციურობა იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

ა) იუმს-ში ჩართული პერსონალისთვის აუცილებელი ცოდნის განსაზღვრა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

გ) სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ ჩანაწერების წარმოება.

2. ორგანიზაციამ უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

მუხლი 13. იუმს-ის მონიტორინგისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა

ორგანიზაციამ უნდა დანერგოს პროცედურები და სხვა კონტროლის მექანიზმები, რაც საშუალებას მისცემს აღმოაჩინოს უსაფრთხოების შემთხვევები და რეაგირება მოახდინოს ინფორმაციული უსაფრთხოების ინციდენტებზე (იხ. დანართი 1, 27001:2011, თავი 4.2.2. თ).

მუხლი 14. რისკების მართვა

1. ორგანიზაციამ უნდა განსაზღვროს რისკების შეფასების მიდგომა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.გ);

2. ორგანიზაციამ უნდა გამოავლინოს რისკები და გაანალიზოს მათი გავლენა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.დ);

3. ორგანიზაციამ უნდა ჩაატაროს გამოვლენილი რისკების ანალიზი და შეფასება (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ე);

4. ორგანიზაციამ უნდა გამოავლინოს და შეაფასოს რისკების მოპყრობის გზები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ვ);

5. ორგანიზაციამ რისკების მოპყრობის მიზნით უნდა შეარჩიოს კონტროლის მიზნები და კონტროლის მექანიზმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.ზ);

6. ორგანიზაციის ხელმძღვანელობამ უნდა დაადასტუროს ნარჩენ რისკებზე თანხმობა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.თ).

მუხლი 15. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

ორგანიზაციამ უნდა მოამზადოს კონტროლის მექანიზმების გამოყენებადობის განაცხადი (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.1.კ), რომელიც შეიცავს:

ა) ამ მოთხოვნების მე-8 მუხლის მე-5 პუნქტში შერჩეულ კონტროლის მიზნებს და კონტროლის მექანიზმებს, ასევე მათი შერჩევის დასაბუთებას;

ბ) ორგანიზაციაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

გ) მგს 27001:2011-ის დანართი ა-დან ნებისმიერი გამორიცხული კონტროლის მიზნის და კონტროლის მექანიზმების ჩამონათვალს და გამორიცხვის დასაბუთებას.

მუხლი 16. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა

1. ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის უახლესი ვერსიის ხელმისაწვდომობა ყველა უფლებამოსილი პირისთვის, ასევე იუმს-ის დოკუმენტაცის სათანადოდ დაცვა და კონტროლი (იხ. დანართი 1, მგს 27001:2011 თავი 4.3.2.).

2. ორგანიზაციამ უნდა აწარმოოს ჩანაწერები და უზრუნველყოს მათი მხარდაჭერა იუმს-ის მოთხოვნებთან შესაბამისობისა და ეფექტიანი ფუნქციონირების მიზნით. ჩანაწერები უნდა იყოს სათანადოდ დაცული და კონტროლდებოდეს (იხ. მგს 27001:2011 თავი 4.3.3).

3. ორგანიზაციის იუმს-ის დოკუმენტაცია მოიცავს (იხ. მგს 27001:2011 თავი 4.3.1):

ა) იუმს-ის პოლიტიკას;

ბ) იუმს-ის გავრცელების სფეროს;

გ) იუმს-ის მხარდამჭერ პროცედურებსა და კონტროლებს;

დ) რისკების შეფასების მეთოდოლოგიის აღწერას;

ე) რისკების შეფასების ანგარიშს;

ვ) რისკების მოპყრობის გეგმას (არ არის სავალდებულო პირველ წელს);

ზ) კონტროლის მექანიზმების ეფექტიანობის საზომების აღწერას (არ არის სავალდებულო პირველ წელს);

თ) ჩანაწერებს;

ი) კონტროლის მექანიზმების გამოყენებადობის განაცხადს.

თავი IV
ორგანიზაციისათვის მესამე წელს შესასრულებელი მოთხოვნები

მუხლი 17. მონიტორინგი

1. ორგანიზაციამ უნდა დანერგოს და განახორციელოს მონიტორინგის და განხილვის პროცედურები, ასევე სხვა კონტროლის მექანიზმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ა), რომელთა მიზანია:

ა) დამუშავების შედეგებში შეცდომების მყისიერი აღმოჩენა;

ბ) უსაფრთხოების გარღვევის მცდელობების და წარმატებული მცდელობების, აგრეთვე ინციდენტების მყისიერი აღმოჩენა;

გ) მიეცეს ხელმძღვანელობას მსჯელობის საშუალება, თუ რამდენად ეფექტიანად მუშაობს უსაფრთხოების ესა თუ ის ღონისძიება;

დ) გამოავლინოს უსაფრთხოების შემთხვევების ინდიკატორების მეშვეობით;

ე) განსაზღვროს, იყო თუ არა გარღვევის მცდელობის აღმოფხვრა ეფექტიანი.

2. ორგანიზაციამ პერიოდულად უნდა განიხილოს იუმს-ის ეფექტიანობა (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვა). პერიოდული მიმოხილვის დროს ორგანიზაციამ უნდა გაითვალისწინოს ინფორმაციული უსაფრთხოების აუდიტის შედეგები, ინციდენტები, ეფექტიანობის გაზომვის შედეგები და დაინტერესებული

მხარეებისგან მიღებული შემოთავაზებები და უკუკავშირი (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ბ).

3. ორგანიზაციამ უნდა გაზომოს კონტროლის მექანიზმების ეფექტიანობა უსაფრთხოების მოთხოვნების დაკმაყოფილების დასადასტურებლად (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.გ).

მუხლი 18. რისკების შეფასების გადახედვა

ორგანიზაციამ დაგეგმილი პერიოდულობით უნდა განახორციელოს რისკების შეფასების, ნარჩენი რისკებისა და რისკების მისაღები დონეების გადახედვა (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.დ), შემდეგი საკითხების გათვალისწინებით:

ა) ორგანიზაციულ-სტრუქტურული ცვლილება;

ბ) ტექნოლოგიური ცვლილება;

გ) ცვლილება საქმიანობის მიზნებსა და პროცესებში;

დ) ახლადაღმოჩენილი საფრთხეები;

ე) დანერგილი კონტროლის მექანიზმების ეფექტიანობის ცვლილება;

ვ) გარე მოვლენები, ისეთი როგორიცაა საკანონმდებლო ცვლილებები;

ზ) შეცვლილი საკონტრაქტო ვალდებულებები და ცვლილებები სოციალურ გარემოში;

მუხლი 19. ორგანიზაციაში იუმს-ის შიდა აუდიტი

1. ორგანიზაცია ვალდებულია ჩაატაროს იუმს-ის აუდიტი (იხ. დანართი 1, მგს 27001:2011 თავი 6) დაგეგმილი პერიოდულობით და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები:

ა) შეესაბამება თუ არა სტანდარტის, საკანონმდებლო მოთხოვნებს;

ბ) შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება თუ არა მისი დანერგვა და მხარდაჭერა;

დ) ფუნქციონირებს თუ არა გეგმის შესაბამისად.

2. ხელმძღვანელობას, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და მათი გამომწვევი მიზეზების აღმოფხვრა. შემდგომი ღონისძიებები გულისხმობს მათ შემოწმებას და შემოწმების შედეგების ანგარიშგებას (იხ. დანართი 1, მგს 27001:2011 თავი 8).

მუხლი 20. ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა

1. ორგანიზაციამ უნდა განახორციელოს იუმს-ის პერიოდული მიმოხილვა, რათა უზრუნველყოფილი იყოს ადეკვატური გავრცელების სფერო და იუმს-ს პროცესის გაუმჯობესებების აღმოჩენა (იხ. დანართი 1, მგს 27001:2011, თავი 7).

2. ხელმძღვანელობა ვალდებულია აწარმოოს იუმს-ს მიმოხილვა დაგეგმილი პერიოდულობით (სულ მცირე წელიწადში ერთხელ) მუდმივი შესაბამისობის, ადექვატურობისა და ეფექტიანობის უზრუნველსაყოფად. მიმოხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვილებების საჭიროებას, მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკას და მიზნებს.

3. მიმოხილვის შედეგები უნდა იყოს დოკუმენტირებული და ხდებოდეს ჩანაწერების წარმოება (იხ. დანართი 1, მგს 27001:2011 თავი 4.3.3).

მუხლი 21. ინფორმაციული უსაფრთხოების ღონისძიებების გეგმების განახლება

ორგანიზაციამ მონიტორინგის და მიმოხილვის შედეგების გათვალისწინებით უნდა განაახლოს ინფორმაციული უსაფრთხოების ღონისძიებების გეგმები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.3.ზ).

მუხლი 22. ორგანიზაციაში იუმს-ის გაუმჯობესება და კომუნიკაცია

ორგანიზაცია ვალდებულია:

ა) იუმს-ში დანერგოს გამოვლენილი გაუმჯობესები (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.4.ა);

ბ) განახორციელოს ყველა დაინტერესებული პირის ინფორმირება გატარებული ქმედებების და გაუმჯობესებების თაობაზე დეტალიზაციის შესაბამისი დონის გათვალისწინებით და, საჭიროების შემთხვევაში, შეათანხმოს შემდგომი ნაბიჯები ინფორმაციული უსაფრთხოების მართვის სისტემაზე პასუხისმგებელ პირებთან (იხ. დანართი 1, მგს 27001:2011, თავი 4.2.4.გ;).

მუხლი 23. იუმს-ის მხარდაჭერა

1. ორგანიზაცია ვალდებულია მუდმივად იზრუნოს იუმს-ის ეფექტიანობის გაუმჯობესებაზე შემდეგი საკითხების გათვალისწინებით:

ა) ინფორმაციული უსაფრთხოების პოლიტიკა და ინფორმაციული უსაფრთხოების მიზნები;

ბ) აუდიტის შედეგები;

გ) მონიტორინგის შედეგად აღმოჩენილი მოვლენების ანალიზი, მაკორექტირებელი და პრევენციული ქმედებები;

დ) ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა (იხ. დანართი 1, მგს 27001:2011 თავი 7).

2. ორგანიზაციამ უნდა:

ა) განახორციელოს მგს 27001:2011-ის 8.2-სა და 8.3-ის თანახმად შესაბამისი მაკორექტირებელი და პრევენციული ქმედებები;

ბ) უზრუნველყოს გაუმჯობესებების შედეგად დასახული მიზნების მიღწევა.

მგს 27001:2011

ინფორმაციული ტექნოლოგიები - უსაფრთხოების საშუალებები - ინფორმაციული უსაფრთხოების მართვის სისტემები - მოთხოვნები

შესავალი

წინამდებარე სტანდარტის მიზანი არის ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში „იუმს“) ჩამოყალიბება, დანერგვა, ფუნქციონირება, ზედამხედველობა, მხარდაჭერა და გაუმჯობესება. იუმს-ის ორგანიზაციაში მიღება სტრატეგიული გადაწყვეტილება უნდა იყოს. ორგანიზაციაში იუმს-ის დიზაინი და დანერგვა განპირობებულია ორგანიზაციის საჭიროებებით და მიზნებით, უსაფრთხოების მოთხოვნებით, არსებული პროცესებით და ორგანიზაციული სტრუქტურით, რომლებიც შესაძლოა დროთა განმავლობაში იცვლებოდეს. მოსალოდნელია, რომ იუმს-ის დანერგვა შეიცვლება ორგანიზაციის საჭიროებების მიხედვით. სტანდარტი შესაძლოა გამოყენებულ იქნეს შესაბამისობის შესამოწმებლად შიდა და გარე დაინტერესებული პირების მიერ.

1. გავრცელების სფერო

1.1.ზოგადი

წინამდებარე სტანდარტი ვრცელდება კრიტიკული ინფორმაციული სისტემის მქონე სუბიექტებზე (შემდეგში ‘‘ორგანიზაციაზე“). სტანდარტი განსაზღვრავს იუმს-ის ჩამოყალიბების, დანერგვის, ფუნქციონიონირების, მონიტორინგის, განხილვის, მხარდაჭერისა და გაუმჯობესების დოკუმენტირებულ მოთხოვნებს ორგანიზაციაში არსებული ზოგადი ბიზნეს-რისკების გათვალისწინებით.

სტანდარტი აღწერს უსაფრთხოების კონტროლის მექანიზმების დანერგვის მოთხოვნებს ყოველი კონკრეტული ორგანიზაციისათვის, ან მისი ნაწილისათვის. იუმს-ის დანიშნულებაა ინფორმაციული აქტივების დამცავი, ადეკვატური და პროპორციული უსაფრთხოების კონტროლის მექანიზმების დანერგვა და დაინტერესებული მხარეების დარწმუნებულობის გამყარება.

შენიშვნა 1: „ბიზნესის“ გამოყენება სტანდარტში უნდა განიხილებოდეს, როგორც ძირითად საქმიანობათა ერთობლიობა, რომელიც აუცილებელია ორგანიზაციის არსებობისათვის.

შენიშვნა 2: სტანდარტი წარმოადგენს დანერგვის სახელმძღვანელოს, რომელიც შესაძლოა გამოყენებულ იქნეს კონტროლის მექანიზმის დიზაინის სტადიაზე.

1.2.გამოყენება

სტანდარტში ჩამოყალიბებული მოთხოვნები არის ზოგადი და უნდა გამოიყენებოდეს ორგანიზაციაში, მიუხედავად მისი სიდიდის, ზომის და ტიპისა. იმისათვის, რომ ორგანიზაცია თავსებადობაში იყოს აღნიშნულ სტანდარტთან, არ დაიშვება 4, 5, 6, 7 და 8 პუნქტებში ჩამოთვლილი არცერთი მოთხოვნის ამოღება. ნებისმიერი კონტროლის მექანიზმის ამოღება, რომელიც აუცილებელია რისკის მისაღებად, უნდა იყოს დაფიქსირებული და გააზრებული და უნდა არსებობდეს მტკიცებულება იმისა, რომ შესაბამისი რისკები მიღებულია პასუხისმგებელი პირების მიერ. სტანდარტთან შესაბამისობა შეუძლებელია, თუ რომელიმე მოთხოვნა ამოღებული იქნება, გარდა იმ შემთხვევებისა, როდესაც ასეთი გამონაკლისები

პირდაპირ არის საკანონმდებლო ან მარეგულირებელ ბაზასთან წინააღმდეგობაში, ან უარყოფითად მოქმედებს ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების მიწოდების შესაძლებლობაზე.

შენიშვნა: იმ შემთხვევაში, როდესაც ორგანიზაციას უკვე გააჩნია ბიზნეს-პროცესის მართვის სისტემა (მაგ. ხარისხის მართვის სისტემები ISO 9001 ან გარემოს მართვის სისტემა ISO 14001), უმეტეს შემთხვევაში სასურველია შესაბამისობა წინამდებარე სტანდარტთან მართვის არსებული სისტემის ფარგლებში.

2. ნორმატიული აქტები

დოკუმენტში დასახელებული სხვა დოკუმენტები წარმოადგენს წინამდებარე სტანდარტის განუყოფელ ნაწილს.

3. ტერმინები და განმარტებები

შენიშვნა: დოკუმენტის ამ ნაწილში მოყვანილი ტერმინები და განმარტებები არ უნდა განიმარტოს „ინფორმაციული უსაფრთხოების შესახებ“ კანონით დადგენილი ანალოგიური ტერმინებისაგან გასხვავებულად, არამედ გამოიყენება როგორც კანონით დადგენილი ტერმინების დამატებითი და დამაზუსტებელი განმარტებები.

3.1.აქტივი

ნებისმიერი რამ, რაც ფასეულია ორგანიზაციისათვის;

3.2.ხელმისაწვდომობა

ავტორიზებული სუბიექტის მიერ მოთხოვნის შესაბამისად ხელმისაწვდომობისა და გამოყენებადობის მახასიათებლები.

3.3.კონფიდენციალურობა

მახასიათებლები იმისა, რომ ინფორმაცია არ არის ხელმისაწვდომი არაავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის;

3.4.ინფორმაციული უსაფრთხოება

ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შენარჩუნება და დაცვა; დამატებით შესაძლოა მოიცავდეს ასევე ისეთ მახასიათებლებს, როგორებიცაა: ავთენტურობა, ანგარიშვალდებულება, წარმოშობის წყაროსთან ცალსახა შესაბამისობა და სანდოობა;

3.5.ინფორმაციული უსაფრთხოების მოვლენა

სისტემის, სერვისისა და ქსელის იდენტიფიცირებული მდგომარეობა, რაც მიუთითებს ინფორმაციული უსაფრთხოების პოლიტიკის შესაძლო დარღვევაზე ან დანერგილი კონტროლის მექანიზმების წარუმატებლობაზე, ან წინასწარ უცნობ ისეთ სიტუაციაზე, რომელიც შესაძლოა მნიშვნელოვანი იყოს უსაფრთხოების თვალსაზრისით;

3.6.ინფორმაციული უსაფრთხოების ინციდენტი

ინფორმაციული უსაფრთხოების მოულოდნელი ან არასასურველი ცალკეული ან სერიული ხდომილებები, რომლებიც დიდი ალბათობით ახდენენ ბიზნეს-ოპერაციების დისკრედიტაციას ან ემუქრებიან ინფორმაციულ უსაფრთხოებას;

3.7. ინფორმაციული უსაფრთხოების მართვის სისტემა - იუმს

მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

3.8 მთლიანობა

აქტივის სიზუსტის და სრულყოფილების დაცვის მახასიათებელი თვისება;

3.9 რეაგირების გარეშე დარჩენილი რისკი

რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

3.10. რისკის მიღება

გადაწყვეტილება რისკის მიღების თაობაზე;

3.11. რისკის ანალიზი

ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მისი შეფასების დასადგენად;

3.12. რისკის შეფასება

რისკის ანალიზისა და რისკის დონის დადგენის სრული პროცესი;

3.13. რისკის დონის დადგენა

რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

3.14. რისკის მართვა

ორგანიზაციის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

3.15. რისკების მოპყრობა

რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

3.16. გამოყენებადობის შესახებ განაცხადი

ორგანიზაციის იუმს-ისთვის საჭირო და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

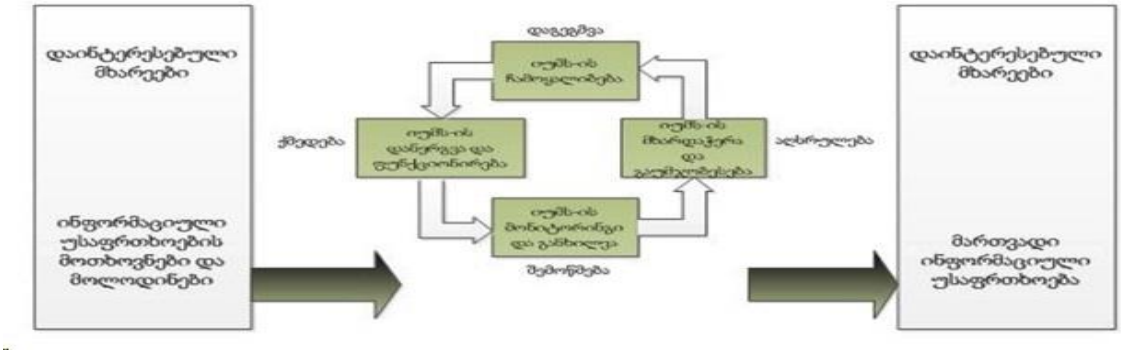
4.ინფორმაციული უსაფრთხოების მართვის სისტემა

4.1.ზოგადი მოთხოვნები

ორგანიზაციამ უნდა ჩამოაყალიბოს

ორგანიზაციამ უნდა ჩამოაყალიბოს, დანერგოს, გამოიყენოს, განახორციელოს მონიტორინგი, განიხილოს, მხარი დაუჭიროს და გააუმჯობესოს დოკუმენტირებული იუმს ორგანიზაციაში ასრებული ყველა ბიზნეს-პროცესის და რისკების

გათვალისწინებით. ამ სტანდარტის მიზნებისთვის გამოიყენება „დაგეგმვა-აღსრულება-შემოწმება-ქმედება“ მოდელი, რომელიც ნაჩვენებია ნახაზზე.



4.2.იუმს-ის ჩამოყალიბება და მართვა

4.2.1.იუმს-ის ჩამოყალიბება

ორგანიზაციამ უნდა შეასრულოს შემდეგი:

ა) განსაზღვროს იუმს-ის გავრცელების სფერო და საზღვრები ბიზნესის, ორგანიზაციის, ადგილმდებარეობის, აქტივების და ტექნოლოგიების ჭრილში, მათ შორის დაასაბუთოს დაშვებული გამონაკლისების მიზეზები (იხილეთ პუნქტი 1.2.)

ბ) განსაზღვროს იუმს პოლიტიკა ბიზნესის, ორგანიზაციის, ადგილმდებარეობის, აქტივების და ტექნოლოგიების ჭრილში, რომელიც:

1. ინფორმაციულ უსაფრთხოებასთან მიმართებაში აყალიბებს მიზნებს, საერთო მიმართულებას და პრინციპებს;

2. ითვალისწინებს საკანონმდებლო და ბიზნესის მარეგულირებელ მოთხოვნებს, აგრეთვე საკონტრაქტო მოთხოვნებს;

3. შეესაბამება ორგანიზაციის სტრატეგიული რისკების მართვის კონტექსტს, რომელშიც მოხდება იუმს-ის ჩამოყალიბება და შენარჩუნება;

4. აყალიბებს რისკების შეფასების კრიტერიუმებს;

5. დამტკიცებულია მენეჯმენტის მიერ.

შენიშვნა: წინამდებარე სტანდარტის მიზნებიდან გამომდინარე იუმს პოლიტიკა განიხილება, როგორც ინფორმაციული უსაფრთხოების პოლიტიკის მომცველი. თუმცა, ეს პოლიტიკები შესაძლოა ერთ დოკუმენტად იყოს ჩამოყალიბებული.

გ) განისაზღვროს ორგანიზაციის რისკების შეფასების მიდგომა.

1.ჩამოყალიბდეს რისკების შეფასების მეთოდოლოგია, რომელიც შესაბამისობაში იქნება იუმს-თან და გაითვალისწინებს ბიზნესის ინფორმაციული უსაფრთხოების, საკანონმდებლო და მარეგულირებელ მოთხოვნებს.

2.შემუშავდეს რისკების მიღების კრიტერიუმები და განისაზღვროს დასაშვები რისკის დონეები.

რისკების შეფასების შერჩეულმა მეთოდოლოგიამ უნდა უზრუნველყოს რისკების შეფასების შედარებადი და განმეორებადი შედეგები.

შენიშვნა: არსებობს რისკების შეფასების სხვადასხვა მეთოდოლოგია. მაგალითები მოყვანილია დოკუმენტში ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security*.

დ) გამოვლინდეს რისკები:

1. გამოვლინდეს იუმს-ის ფარგლებში აქტივები და მათი მფლობელები*;

2. გამოვლინდეს ამ აქტივებთან დაკავშირებული საფრთხეები;

3. გამოვლინდეს სისუსტეები, რომელებითაც შესაძლოა ისარგებლონ საფრთხეებმა;

4.გამოვლინდეს აქტივებზე კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევით გამოწვეული დანაკარგები.

შენიშვნა: ტერმინი „მფლობელი“ გამოიყენება ინდივიდის ან ობიექტის აღსაწერად, რომელსაც გააჩნია აქტივის წარმოების, შენარჩუნების ან დაცვის მოვალეობა. „მფლობელი“ არ ნიშნავს იმას, რომ პიროვნებას გააჩნია აქტივზე საკუთრების უფლება.

ე) გააანალიზოს და შეაფასოს რისკები.

1. შეფასდეს ორგანიზაციის ბიზნესისთვის უსაფრთხოების დარღვევით გამოწვეული შედეგი კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევის გათვალისწინებით;

2. შეფასდეს უსაფთხოების დარღვევის ხდომილების ალბათობა ჭარბი საფრთხეების და სისუსტეების შემთხვევაში, აქტივებზე მათი შედეგები და არსებული კონტროლის მექანიზმები.

3. შეფასდეს რისკის დონეები.

4. განისაზღვროს, მოხდება თუ არა რისკის მიღება და საჭიროებს თუ არა 4. რისკი მოპყრობას რისკების მიღების კრიტერიუმების შესაბამისად (იხ.4.2.1გ)2).

ვ) აღმოჩენილ იქნეს და შეფასდეს რისკების მიღების ნაირსახეობები. შესაძლო ქმედებები არის:

1.შესაბამისი კონტროლის მექანიზმების გამოყენება;

2.გაცნობიერებულად და ობიექტურად რისკის მიღება ორგანიზაციის პოლიტიკების და რისკების მიღების კრიტერიუმების გათვალისწინებით;

3.რისკის თავიდან აცილება.

4.რისკის გადატანა სხვა მხარეებზე, მაგალითად დაზღვევა, მომწოდებლები.

ზ) რისკების სამართავად უნდა მოხდეს კონტროლის მიზნების და კონტროლის მექანიზმების შერჩევა, რომელიც უნდა შეესაბამებოდეს რისკების შეფასების და რისკების მოპყრობის პროცესს. შერჩევა უნდა ეფუძნებოდეს რისკების მიღების კრიტერიუმებს (იხ 4.2.1 გ)2)), აგრეთვე საკანონმდებლო, მარეგულირებელ და საკონტრაქტო მოთხოვნებს.

დანართში ა მოცემული კონტროლის მიზნები და კონტროლის მექანიზმები უნდა იყოს ამ პროცესის შემადგენელი. თუმცა, **დანართში ა** მოცემული კონტროლის

მექანიზმები და კონტროლის მიზნები არ წარმოადგენს ამომწურავ ჩამონათვალს, ამიტომ შესაძლებელია შეირჩეს დამატებითი კონტროლის მექანიზმები.

შენიშვნა: დანართი ა წარმოადგენს კონტროლის მექანიზმების და კონტროლის მიზნების ზოგად ჩამონათვალს. წინამდებარე სტანდარტის მომხმარებლები განიხილავენ დანართ ა-ს კონტროლის მექანიზმების შერჩევის საწყის წერტილად, რათა არ მოხდეს მნიშვნელოვანი კონრტოლის მექანიზმების გამოტოვება.

თ) რეაგირების გარეშე დარჩენილი რისკების შესახებ მენეჯმენტისგან თანხმობის მიღება.

ი) იუმს-ის დანერგვასა და ფუნქციონირების თაობაზე მენეჯმენტისგან თანხმობის მიღება.

კ) გამოყენებადობის შესახებ განაცხადი უნდა მომზადდეს და ძირითადად უნდა შეიცავდეს:

1. კონტროლის მიზნებს და 4.2.1თ) -ში შერჩეულ კონტროლის მექანიზმებს და მათი შერჩევის მიზეზებს;

2. არსებული კონტროლების მიზნებს და კონტროლის მექანიზმებს (იხ.4.2.1 ე)2);

3. ნებისმიერი კონტროლის მიზნების და კონტროლის მექანიზმების ამოღებას დანართი ა-დან და ამოღების დასაბუთებას.

შენიშვნა: გამოყენებადობის შესახებ განაცხადი წარმოადგენს გადაწყვეტილებათა შეჯამებას რისკებთან მოპყრობის შესახებ. გამონაკლისების ახსნა კიდევ ერთი შემოწმების საშუალებაა იმისა, რომ არაფერი გამოგვრჩა მნიშვნელოვანი.

4.2.2.იუმს-ის დანერგვა და ფუნქციონირება

ორგანიზაციამ უნდა შეასრულოს შემდეგი:

ა) ჩამოაყალიბოს რისკთან მოპყრობის გეგმა, რომელიც აღწერს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო მენეჯმენტის ქმედებებს, რესურსებს, პასუხისმგებლობებს და პრიორიტეტებს (იხილეთ პუნქტი 5).

ბ) დანერგოს რისკების მოპყრობის გეგმა, რათა მოხდეს კონტროლის მიზნების მიღწევა, რაც გულისხმობს სახსრების განაწილებას და პასუხისმგებლობების და როლების განსაზღვრას.

გ) დაინერგოს 4.2.1 ზ-ში ნახსენები კონტროლის მექანიზმები, რათა მოხდეს კონტროლის მიზნების მიღწევა.

დ) განისაზღვროს შერჩეული კონტროლის მექანიზმების ან კონტროლის მექანიზმების ჯგუფის ეფექტიანობის გაზომვის საშუალებები და დადგინდეს თუ როგორ მოხდება ამ საზომების გამოყენება (4.2.3გ).

შენიშვნა: კონტროლის მექანიზმის ეფექტიანობის გაზომვა მენეჯერებს და პერსონალს საშუალებას აძლევს განსაზღვრონ, შერჩეული კონტროლის მექანიზმი რამდენად ეფექტიანად იძლევა კონტროლის მიზნების მიღწევის საშუალებას.

ე) დაინერგოს სატრენინგო და ცნობიერების ამაღლების პროგრამები (იხილეთ 5.2.2.);

ვ) მართოს იუმს ფუნქციონირება;

ზ) მართოს იუმს რესურსები (იხილეთ 5.2);

თ) დანერგოს პროცედურები და სხვა კონტროლის მექანიზმები, რომლებიც დაეხმარება უსაფრთხოების მოვლენების აღმოჩენაში და ამ ინციდენტებზე რეაგირებაში (იხილეთ 4.2.3. ა)).

4.2.3.იუმს-ის მონიტორინგი და განხილვა

ორგანიზაცია ვალდებულია:

ა) განახორციელოს მონიტორინგი და განხილვის პროცედურები და სხვა კონტროლის მექანიზმები, რათა:

1.დამუშავების შედეგებში დაუყოვნებლივ აღმოაჩინოს შეცდომები;

2.დაუყოვნებლივ აღმოაჩინოს უსაფრთხოების გარღვევის მცდელობები, ინციდენტები და შედეგები;

3.მისცეს მენეჯმენტს მსჯელობის საშუალება, თუ რამდენად ეფექტიანად მუშაობს ესა თუ ის უსაფრთხოების კონტროლის მექანიზმები;

4.დაეხმაროს უსაფრთხოების მოვლენების აღმოჩენაში და ინდიკატორების მეშვეობით უსაფრთხოების ინციდენტების თავიდან აცილებაში;

5.განსაზღვროს, იყო თუ არა გარღვევის მცდელობის აღმოფხვრა შედეგიანი.

ბ) აწარმოოს იუმს ეფექტიანობის პერიოდული მიმოხილვა (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვა) უსაფრთხოების აუდიტების, ინციდენტების, ეფექტიანობის გაზომვის შედეგების გათვალისწინებით და დაინტერესებული მხარეებისგან შემოთავაზებების და უკუკავშირის გათვალისწინებით.

გ) გაზომოს კონტროლის მექანიზმების ეფექტიანობა უსაფრთხოების მოთხოვნების დაკმაყოფილების შესამოწმებლად;

დ) განახორციელოს რისკების შეფასების განხილვა დროის დაგეგმილ ინტერვალებში, რეაგირების გარეშე დარჩენილი რისკების და რისკების მისაღები დონის განხილვა, შემდეგი ცვლილებების გათვალისწინებით:

1.ორგანიზაცია;

2.ტექნოლოგია;

3.ბიზნესის მიზნები და პროცესები;

4.აღმოჩენილი საფრთხეები;

5.დანერგილი კონტროლის მექანიზმების ეფექტიანობა;

6.გარე მოვლენები, ისეთი როგორც საკანონმდებლო და მარეგულირებელი ცვლილებები, შეცვლილი საკონტრაქტო ვალდებულებები და ცვლილებები სოციალურ გარემოში;

ე) განხორციელდეს იუმს-ის პერიოდული აუდიტები (იხილეთ პუნქტი 6).

შენიშვნა: შიდა აუდიტების განხორციელება ხდება ორგანიზაციის მიერ ან ორგანიზაციის სახელით, შიდა მიზნებიდან გამომდინარე.

ვ) განხორციელდეს იუმს-ის პერიოდული განხილვა, რათა უზურნველყოფილი იყოს ადექვატური გავრცელების სფერო და იუმს-ის პროცესის გაუმჯობესებების აღმოჩენა (იხ 7.1);

ზ) განაახლოს უსაფრთხოების გეგმები მონიტორინგის დაკვირვებების და განხილვის შედეგების გათვალისწინებით;

თ) ქმედებების და მოვლენების დაფიქსირება, რომლებმაც შეიძლება გავლენა იქონიოს იუმს-ის ეფექტიანობაზე ან წარმადობაზე (იხ. 4.3.3).

4.2.4.იუმს-ის შენარჩუნება და გაუმჯობესება

ორგანიზაცია ვალდებულია პერიოდულად განახორციელოს:

ა) აღმოჩენილი გაუმჯობესების იუმს-ში დანერგვა;

ბ) 8.2 და 8.3 თანახმად განახორციელოს შესაბამისი მაკორექტირებელი და პრევენციული ქმედებები. გამოიყენოს სხვა ორგანიზაციების და საკუთარი გამოცდილება ამ საკითხში.

გ) მოახდინოს ყველა დაინტერესებული პირის შეტყობინება განხორციელებული ქმედებების და გაუმჯობესებების თაობაზე ვითარების შესაბამისი დეტალიზაციის დონის გათვალისწინებით და შეათანხმოს შემდგომი ნაბიჯები.

დ) უზრუნველყოს დაგეგმილი მიზნების რეალიზაცია გაუმჯობესებების მეშვეობით.

4.3.დოკუმენტაციის მოთხოვნები

4.3.1.ზოგადი

დოკუმენტაცია უნდა შეიცავდეს ჩანაწერებს მენეჯერული გადაწყვეტილებების შესახებ, უზრუნველყოს მოქმედებების ცალსახა იდენტიფიცირება მენეჯერულ გადაწყვეტილებებთან და პოლიტიკებთან და უზრუნველყოს დაფიქსირებული შედეგების განმეორებადობა. მნიშვნელოვანია ურთიერთკავშირის დამყარება შერჩეულ კონტროლის მექანიზმებსა და რისკების შეფასების და რისკების მოპყრობის პროცესებს შორის, აგრეთვე იუმს პოლიტიკასა და მიზნებთან. იუმს დოკუმენტაცია უნდა შეიცავდეს:

ა) იუმს-ის პოლიტიკის დოკუმენტირებულ ფორმულირებას (4.2.1 ბ) და მიზნებს;

ბ) იუმს-ის გავრცელების სფეროს (4.2.1 ა);

გ) იუმს-ის მხარდამჭერ პროცედურებსა და კონტროლის მექანიზმებს;

დ) რისკების შეფასების მეთოდოლოგიის აღწერას (4.2.1 გ);

ე) რისკების შეფასების ანგარიშს (4.2.1 გ-დან 4.2.1 ზ-მდე);

ვ) რისკების მოპყრობის გეგმას (4.2.2 ბ);

ზ) უსაფრთხოების პოლიტიკის პროცესების ეფექტიანი დაგეგმარებისა, ფუნქციონირების და კონტროლისათვის აუცილებელ ორგანიზაციულ დოკუმენტირებულ პროცედურებს და აღიწეროს, თუ როგორ უნდა განხორციელდეს კონტროლის მექანიზმების ეფექტიანობის გაზომვა (4.2.3 გ);

თ) წინამდებარე სტანდარტით აუცილებელ ჩანაწერებს (4.3.3);

ი) გამოყენებადობის შესახებ განაცხადს.

შენიშვნა 1: ტერმინი „დოკუმენტირებული პროცედურა“ გამოიყენება წინამდებარე სტანდარტში, ნიშნავს, რომ პროცედურა არის ჩამოყალიბებული, დოკუმენტირებული, დანერგილი და მხარდაჭერილი.

შენიშვნა 2: იუმს დოკუმენტაციის დაწვრილმანება შესაძლოა ვარირებდეს სხვადასხვა ორგანიზაციაში შემდეგის გათვალისწინებით:

- ორგანიზაციის სიდიდე და მისი საქმიანობის ტიპი;
- უსაფრთხოების მოთხოვნების და მართვის სისტემის გავრცელების სფერო და სირთულე;

შენიშვნა 3: დოკუმენტები და ჩანაწერები შესაძლოა იყოს ინფორმაციის ნებისმიერი სახის ან ტიპის მატარებელზე.

4.3.2.დოკუმენტებზე კონტროლი

იუმს-ის მიერ მოთხოვნილი დოკუმენტები უნდა იყოს დაცული. ჩამოსაყალიბებელი დოკუმენტირებული პროცედურა განისაზღვრავს მენეჯმენტის შემდეგ ქმედებებს:

ა) დოკუმენტის გამოქვეყნებამდე მისი დადასტურება;

ბ) დოკუმენტების განხილვა და ცვლილება აუცილებლობის შემთხვევაში და მისი თავიდან დადასტურება;

გ) უზრუნველყოს დოკუმენტების მიმდინარე ვერსიისა და ცვლილებების დაფიქსირება;

დ) უზრუნველყოს დოკუმენტის სხვადასხვა ვერსიების ხელმისაწვდომობა საჭიროების შემთხვევაში;

ე) უზრუნველყოს, რომ დოკუმენტები არის ჩამოყალიბებული მკაფიოდ და ცალსახად იდენტიფიცირებადია;

ვ) უზრუნლველყოს დოკუმენტების ხელმისაწვდომობა ყველა უფლებამოსილი მხარისათვის და მათი გადაადგილების, შენახვის და განადგურების არსებულ კლასიფიცირების პროცედურებთან შესაბამისობა.

ზ) უზრუნველყოს გარე წარმოშობის დოკუმენტების იდენტიფიცირება;

თ) უზრუნველყოს დოკუმენტების განაწილებაზე კონტროლი;

ი) აიკრძალოს ძველი დოკუმენტების არასათანადოდ გამოყენება, და;

კ) ნებისმიერი მიზნით შენახვის შემთხვევაში გამოიყენებოდეს სათანადო იდენტიფიცირება;

4.3.3. ჩანაწერთა კონტროლი

ჩანაწერები უნდა შეიქმნას და შენარჩუნდეს, რათა უზრუნველყოფილი იყოს იუმს-ის მოთხოვნებთან შესაბამისობა და ეფექტიანი ფუნქციონირება. ჩანაწერები უნდა იყოს დაცული და კონტროლდებოდეს. იუმს-მა უნდა გაითვალისწინოს ნებისმიერი საკანონმდებლო, მარეგულირებელი ან სახელშეკრულებო ვალდებულება. ჩანაწერები უნდა იყოს მკაფიო, იდენტიფიცირებადი და ხელმისაწვდომი. იდენტიფიცირების, შენახვის, დაცვის, ხელმისაწვდომობის, განადგურების ვადის და განთავსებისთვის საჭირო კონტროლის მექანიზმები უნდა

იყოს აღწერილი და დანერგილი. პროცესის წარმადობის და იუმს-ის ყველა უსაფრთხოების ინციდენტის შესახებ ჩანაწერების შენახვა უნდა მოხდეს 4.2-ს მიხედვით.

მაგალითი: ჩანაწერთა მაგალითი შესაძლოა იყოს ვიზიტორების სარეგისტრაციო ჟურნალი, აუდიტის ანგარიში და წვდომის დაშვების ფორმა.

5.მენეჯმენტის პასუხისმგებლობა

5.1. მენეჯმენტის მზადყოფნა

მენეჯმენტი ვალდებულია წარადგინოს მზადყოფნის შესახებ მტკიცებულება იუმს-ის ჩამოყალიბებაზე, დანერგვაზე, ფუნქციონირებაზე, მონიტორინგზე, განხილვაზე, შენარჩუნებაზე და გაუმჯობესებაზე შემდეგი ჩამონათვლის გათვალისწინებით:

ა) იუმს პოლიტიკის ჩამოყალიბებით;

ბ) იუმს მიზნების და გეგმების ჩამოყალიბებით;

გ) ინფორმაციული უსაფრთხოების როლების და პასუხისმგებლობების ჩამოყალიბებით;

დ) ორგანიზაციისადმი ინფორმაციული უსაფრთხოების მიზნების და პოლიტიკის მნიშვნელობის, მისი საკანონმდებლო პასუხისმგებლობის და მუდმივი გაუმჯობესების აუცილებლობის ახსნით;

ე) იუმს-ის ჩამოსაყალიბებლად, დასანერგად, ფუნქციონირებისათვის, მონიტორინგისათვის, შენარჩუნებისათვის, განხილვისათვის და გაუმჯობესებისათვის საკმარისი რესურსების გამოყოფა (იხილეთ 5.2.1);

ვ) განსაზღვროს რისკის მიღების და დასაშვები რისკის დონეების კრიტერიუმები;

ზ) უზრუნველყოს იუმს-ის შიდა აუდიტების წარმოება (იხ.6);

თ) მოახდინოს იუმს-ის მენეჯერული განხილვა (იხ.7).

5.2. რესურსების მართვა

5.2.1. რესურსებით უზრუნველყოფა

ორგანიზაცია ვალდებულია განსაზღვროს და გამოყოს აუცილებელი რესურსები, რათა მოხდეს:

ა) იუმს ჩამოყალიბება, დანერგვა, ფუნქციონირება, მონიტორინგი, შენარჩუნება, განხილვა და გაუმჯობესება;

ბ) ინფორმაციული უსაფრთხოების პროცედურების მიერ ბიზნეს მოთხოვნების მხარდაჭერა;

გ) საკანონმდებლო და მარეგულირებელი მოთხოვნების და სახელშეკრულებო ვალდებულებების გამოვლენა და დაკმაყოფილება;

დ) ყველა დანერგილი კონტროლის მექანიზმის სათანადო გამოყენებით ადექვატური უსაფრთხოების შენარჩუნება;

ე) საჭიროების შემთხვევაში განხილვა და განხილვის შედეგად შესაბამისი რეაგირება;

ვ) იუმს-ის ეფექტიანობის გაუმჯობესება, სადაც ეს მიზანშეწონილი იქნება.

5.2.2. სწავლება, ინფორმირება და ცნობიერების ამაღლება

ორგანიზაციამ უდა უზრუნველყოს იუმს-ისთან მიმართებაში პერსონალის კვალიფიციურობა შემდეგი საქმიანობის შესრულებით:

ა) განისაზღვროს იუმს-ში ჩართული პერსონალის აუცილებელი ცოდნა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. მცოდნე პერსონალის აყვანა) საჭიროებების დასაკმაყოფილებლად;

გ) განხორციელებული ქმედებების ეფექტიანობის შეფასება;

დ) სწავლების, ტრენინგის, ცოდნის, გამოცდილების და კვალიფიკაციის შესახებ ინფორმაციის დაგროვება;

ორგანიზაციამ აგრეთვე უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელობას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

6.იუმს-ის შიდა აუდიტები

ორგანიზაცია ვალდებულია ჩაატაროს იუმს აუდიტი დაგეგმილ დროის ინტერვალებში და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები:

ა) შეესაბამება სტანდარტის, საკანონმდებლო და მარეგულირებელ მოთხოვნებს;

ბ) შეესაბამება გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება მისი დანერგვა და შენარჩუნება;

დ) მოქმედებს დაგეგმილის შესაბამისად.

აუდიტის პროგრამა უნდა დაიგეგმოს პროცესების და არეების მნიშვნელობის და სტატუსის გათვალისწინებით, აგრეთვე წინა აუდიტის შედეგების გათვალისწინებით. უნდა განისაზღვროს აუდიტის კრიტერიუმები, გავრცელების სფერო, სიხშირე და მიდგომა. აუდიტორების შერჩევამ და აუდიტის წარმოებამ უნდა უზრუნველყოს აუდიტის პროცესის ობიექტურობა და დამოუკიდებლობა. აუდიტორებმა არ უნდა შეამოწმონ საკუთარი ნამუშევარი. აუდიტის დაგეგვის და წარმოების უფლება-მოვალეობები და მოთხოვნები, აგრეთვე ანგარიშგების შედეგები უნდა განისაზღვროს დოკუმენტირებული პროცედურის მიერ (იხ. 4.3.3). მენეჯმენტს, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და გამომწვევი მიზეზების დაუყოვნებლივი აღმოფხვრა. გამოსწორების შემდეგ უნდა მოხდეს მისი შემოწმება და შემოწმების შედეგების შესახებ ანგარიშგება (იხ. 8).

შენიშვნა: ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*წარმოადგენს სასარგებლო სახელმძღვანელოს იუმს-ის შიდა აუდიტის წარმოებისათვის.

7.იუმს-ის მენეჯერული განხილვა

7.1. ზოგადი

მენეჯმენტი ვალდებულია აწარმოოს იუმს-ის განხილვა დაგეგმილ დროის ინტერვალებში (სულ ცოტა წელიწადში ერთხელ) მიმდინარე შესაბამისობის, ადექვატურობისა და ეფექტიანობის უზრუნველსაყოფად. განხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვილებების აუცილებლობას, ინფორმაციული უსაფრთხოების პოლიტიკისა და მიზნების გათვალისწინებით. განხილვის შედეგები ცალსახად უნდა იყოს დოკუმენტირებული და ჩანაწერები უნდა შენარჩუნდეს (იხ 4.3.3).

7.2. განსახილველი საკითხების ჩამონათვალი

მენეჯერული განხილვისთვის საჭირო საკითხები უნდა მოიცავდეს:

ა) იუმს-ის აუდიტის შედეგებს და განხილვებს;

ბ) დაინტერესებულ პირთა უკუკავშირს;

გ) იუმს წარმადობისა და ეფექტიანობის გაუმჯობესების ტექნიკას, პროდუქტს ან პროცედურას;

დ) პრევენციული ან მაკორექტირებელი ქმედებების სტატუსს;

ე) რისკების წინა შეფასების დროს არასათანადოდ რეაგირებულ სისუსტეებს ან საფრთხეებს;

ვ) ეფექტიანობის გაზომვის შედეგებს;

ზ) წინა სამენეჯერო განხილვის შემდგომ განხორციელებულ ქმედებებს;

თ) ნებისმიერ ცვლილებას, რომელმაც შესაძლოა გავლენა იქონიოს იუმს-ზე;

ი) გაუმჯობესების რეკომედაციებს.

7.3.განხილვის შედეგი

მენეჯერული განხილვის შედეგი უნდა მოიცავდეს ნებისმიერ გადაწყვეტილებას და ქმედებას შემდეგ საკითხებთან მიმართებაში:

ა) იუმს-ის ეფექტიანობის გაუმჯობესებას;

ბ) რისკების შეფასების და რისკების მოპყრობის გეგმის განახლებას;

გ) ინფორმაციული უსაფრთხოების პროცედურების და კონტროლის მექანიზმის ცვლილებას, რომელიც იუმს-ის შიდა ან გარე ფაქტორებისგან დაცვას ემსახურება, მათ შორის:

1.ბიზნეს მოთხოვნები;

2.უსაფრთხოების მოთხოვნები;

3.არსებულ ბიზნეს მოთხოვნებთან დაკავშირებული ბიზნეს-პროცესები;

4.მარეგულირებელი ან საკანონმდებლო მოთხოვნები;

5.საკონტრაქტო ვალდებულებები;

6.რისკის დონეები ან/და რისკის მიღების კრიტერიუმები;

დ) საჭირო რესურსები;

ე) კონტროლის მექანიზმების ეფექტიანობის შეფასების გაუმჯობესება.

8. იუმს-ის გაუმჯობესება

8.1.უწყვეტი გაუმჯობესება

ორგანიზაცია ვალდებულია მუდმივად გააუმჯობესოს იუმს-ის ეფექტიანობა ინფორმაციული უსაფრთხოების პოლიტიკის, ინფორმაციული უსაფრთხოების მიზნების, აუდიტის შედეგების, მონიტორინგის შედეგად აღმოჩენილი მოვლენების ანალიზის, მაკორექტირებელი და პრევენციული ქმედებების და მენეჯერული განხილვის გზით (იხ. 7).

8.2. მაკორექტირებელი ქმედება

ორგანიზაცია ვალდებულია იუმს-ის მოთხოვნებთან შეუსაბამობების შემთხვევაში განახორციელოს გარკვეული ქმედება, რათა თავიდან აიცილოს ფაქტის განმეორება. მაკორექტირებელი ქმედების დოკუმენტირებული პროცედურა უნდა განსაზღვრავდეს:

ა) შეუსაბამობების აღმოჩენას;

ბ) შეუსაბამობების მიზეზების გამოვლენას;

გ) შეაფასოს ქმედების საჭიროება, რათა არ მოხდეს შეუსაბამობის განმეორება;

დ) გამოავლინოს და დანერგოს მაკორექტირებელი ქმედება;

ე) განხორციელებული ქმედების შედეგების დაფიქსირებას (იხ. 4.3.3);

ვ) მაკორექტირებელი ქმედების განხილვას.

8.3.პრევენციული ქმედება

ორგანიზაციამ უნდა განსაზღვროს იუმს-ის მოთხოვნებთან პოტენციური შეუსაბამობის აღმოსაფხვრელად საჭირო ქმედება, რათა თავიდან აიცილოს მათი დადგომა ან განმეორება. პრევენციული ქმედება პოტენციური პრობლემის შესაბამისი უნდა იყოს. პრევენციული ქმედების შესაბამისი დოკუმენტირებული პროცედურა უნდა განსაზღვრავდეს მოთხოვნებს შემდეგი საკითხებისთვის:

ა) პოტენციური შეუსაბამობის აღმოჩენა და მათ მიზეზები;

ბ) ქმედების საჭიროების შეფასება შეუსაბამობის თავიდან ასაცილებლად;

გ) პრევენციული ქმედების გამოვლენა და დანერგვა;

დ) განხორციელებული ქმედების შედეგის შესახებ ჩაწერის გაკეთება (იხ. 4.3.3);

ე) გატარებული პრევენციული ღონისძიების განხილვა.

ორგანიზაცია ვალდებულია გამოავლინოს შეცვლილი რისკები და პრევენციული ქმედებების მოთხოვნები, მნიშვნელოვანწილად შეცვლილ რისკებზე ყურადღების გამახვილებით. პრევენციული ქმედებების პრიორიტეტულობა უნდა განისაზღვრებოდეს რისკების შეფასების საფუძველზე.

შენიშვნა: ხშირად პრევენციული ქმედება უფრო ეფექტიანია ხარჯების მხრივ, ვიდრე მაკორექტირებელი ქმედება.

დანართი ა
ნორმატიული

კონტროლის მიზნები და კონტროლის მექანიზმები

ა.1 ცხრილში ჩამოთვლილი კონტროლის მიზნები და კონტროლის მექანიზმები პირდაპირ გამომდინარეობს და დაკავშირებულია მგს 27002:2011 სტანდარტის 5-დან 15-მდე პუნქტებთან. ცხრილის ჩამონათვალი არ არის სრულყოფილი და ორგანიზაციამ შესაძლოა ჩათვალოს, რომ საჭირო არის დამატებითი კონტროლების მიზნები და კონტროლის მექანიზმები. კონტროლის მიზნები და კონტროლის მექანიზმები ამ ცხრილიდან უნდა შეირჩეს როგორც 4.2.1-ში აღწერილი იუმს-ის პროცესის ნაწილი. მგს 27002:2011 სტანდარტის პუნქტები 5-დან 15-მდე წარმოადგენს დანერგვის სახელმძღვანელოს საუკეთესო პრაქტიკებიდან.

ცხრილი ა.1 - კონტროლის მიზნები და კონტროლის მექანიზმები

ა.5 უსაფრთხოების პოლიტიკა		
ა.5.1 ინფორმაციული უსაფრთხოების პოლიტიკა *მიზანი:* მოხდეს მენეჯმენტის მიმართვა და მხარდაჭერა ინფორმაციული უსაფრთხოების საკითხში ბიზნესის და საკანონმდებლო და მარეგულირებელ მოთხოვნებთან შესაბამისად.		
ა 5.1.1	ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტი	*კონტროლის მექანიზმი:* ინფორმაციული პოლიტიკა უნდა იყოს დამტკიცებული მენეჯმენტის მიერ და უნდა გამოქვეყნდეს და მიეწოდოს ყველა თანამშრომელს და გარე დაინტერესებულ მხარეს.
ა 5.1.2	ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა	*კონტროლის მექანიზმი:* ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა უნდა ხდებოდეს წინასწარ განსაზღვრულ დროის ინტერვალებში ან მნიშვნელოვანი ცვლილებების შემთხვევაში, რათა უზრუნველყოფილი იყოს მისი ვარგისიანობა, ადეკვატურობა და ეფექტიანობა.
ა.6 ინფორმაციული უსაფრთხოების ორგანიზება		
ა.6.1 შიდა ორგანიზება *მიზანი:* ორგანიზაციაში ინფორმაციული უსართხოების მართვა		
ა 6.1.1	ინფორმაციული უსაფრთხოებისადმი მენეჯმენტის მზადყოფნა	*კონტროლის მექანიზმი:* მენეჯმენტი ვალდებულია ორგანიზაციაში აქტიურად დაუჭიროს მხარი უსაფრთხოებას.

ა 6.1.2	ინფორმაციული უსაფრთხოების კოორდინირება	*კონტროლის მექანიზმი:* ინფორმაციული უსაფრთხოების საქმიანობები კოორდინირებული უნდა იყოს ორგანიზაციის სხვადასხვა ქვედანაყოფში შესაბამისი როლების და სამუშაოს გათვალისწინებით.
ა 6.1.3	ინფორმაციული უსაფრთხოების პასუხისმგებლობების განაწილება	*კონტროლის მექანიზმი:* ინფორმაციული უსაფრთხოების პასუხისმგებლობები ცალსახად უნდა იყოს განსაზღვრული.
ა 6.1.4	ინფორმაციის დამუშავების საშუალებათა ავტორიზაციის პროცესი	*კონტროლის მექანიზმი:* ყოველი ახალი ინფორმაციის დამუშავების საშუალებისადმი ავტორიზაცია უნდა იყოს განსაზღვრული და დანერგილი მენეჯმენტის მიერ.
ა 6.1.5	შეთანხმებები კონფიდენციალურობის შესახებ	*კონტროლის მექანიზმი:* ორგანიზაციაში ინფორმაციული უსაფრთხოების ამსახავი შეთანხმებები კონფიდენციალურობის და გაუმჟღავნებლობის შესახებ უნდა განისაზღვროს და პერიოდულად გადაიხედოს.
ა 6.1.6	კავშირი ხელისუფლებასთან	*კონტროლის მექანიზმი:* უნდა დამყარდეს ფორმალიზებული კავშირი შესაბამის მარეგულირებელ სახელმწიფო ინსტიტუტებთან
ა 6.1.7	კავშირი სპეციალურ დაინტერესებულ ჯგუფებთან	*კონტროლის მექანიზმი:* მოხდეს სპეციალურ დაინტერესებულ ჯგუფებთან და სპეციალისტთა უსაფრთხოების ფორუმებთან და პროფესიულ ასოციაციებთან ურთიერთობის შენარჩუნება.
ა 6.1.8	ინფორმაციული უსაფრთხოების დამოუკიდებელი განხილვა.	*კონტროლის მექანიზმი:* ინფორმაციული უსაფრთხოების მართვისადმი ორგანიზაციული მიდგომა და მისი დანერგვა (მაგ. ინფორმაციული უსაფრთხოების კონტროლის მიზნები, კონტროლის მექანიზმები, პოლიტიკები, პროცესები და პროცედურები) უდნა გადაიხედოს დამოუკიდებლად წინასწარ დაგეგმილ დროის ინტერვალებში, ან როდესაც მოხდება უსაფრთხოებაში მნიშვნელოვანი ცვლილება.
ა.6.2 მესამე მხარეები *მიზანი:* ორგანიზაციის ინფორმაციისა და მისი დამუშავების საშუალებების უსაფრთხოების შენარჩუნება, როდესაც მათზე წვდომა მესამე მხარის მიერ ხორციელდება		

ა 6.2.1	მესამე მხარეებთან დაკავშირებული რისკების აღმოჩენა	*კონტროლის მექანიზმი:* ორგანიზაციის და მესამე მხარის მიერ წვდომად, დამუშავებულ, მიწოდებულ და მართვად ინფორმაციასთან დაკავშირებული რისკები უნდა იქნეს გამოვლენილი და დაინერგოს შესაბამისი კონტროლის მექანიზმები, წვდომის უფლების მინიჭებამდე.
ა 6.2.2	კლიენტებთან ურთიერთობისას უსაფრთხოების ზომების მიღება	*კონტროლის მექანიზმი:* უსაფრთხოების მოთხოვნების შესაბამისი ყველანაირი ზომა უნდა იქნეს მიღებული, კლიენტების მხრიდან ორგანიზაციის ინფორმაციაზე ან აქტივებზე წვდომამდე.
ა 6.2.3	მესამე მხარეებთან შეთანხმებების დროს უსაფრთხოების ზომების მიღება	*კონტროლის მექანიზმი:* მესამე მხარეებთან შეთანხმებამ უნდა მოიცვას უსაფრთხოების ყველა შესაბამისი საკითხი, როდესაც ხდება მესამე მხარის მიერ ინფორმაციის დამუშავების საშუალებების ან ინფორმაციის წვდომა, დამუშავება, მასთან დაკავშირება ან მართვა.
ა.7 აქტივების მართვა		
ა.7.1 პასუხისმგებლობა აქტივებზე *მიზანი:* ორგანიზაციული აქტივების სათანადოდ დაცვა და შენარჩუნება		
ა 7.1.1	აქტივების ინვენტარიზაცია	*კონტროლის მექანიზმი:* ყველა აქტივი უნდა აღიწეროს და მოხდეს მნიშვნელოვანი აქტივების ინვენტარიზაცია
ა 7.1.2	აქტივების მფლობელობა	*კონტროლის მექანიზმი:* ყველა ინფორმაცია და ინფორმაციის დამუშავების საშუალებებთან დაკავშირებული ყველა აქტივი უნდა იყოს ორგანიზაციის გარკვეული ერთეულის მფლობელობაში
ა 7.1.3	აქტივების სათანადო გამოყენება	*კონტროლის მექანიზმი:* ინფორმაციის და ინფორმაციის დამუშავებასთან დაკავშირებული აქტივების დასაშვები მართვის წესები უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და დანერგვა.
ა.7.2 ინფორმაციის კლასიფიცირება *მიზანი:* ინფორმაციის სათანადო დაცვის დონის უზრუნველყოფა		
ა 7.2.1	კლასიფიკაციის სახელმძღვანელო	*კონტროლის მექანიზმი:* ინფორმაციის კლასიფიკაცია უნდა მოხდეს მისი ორგანიზაციაში ღირებულების, საკანონმდებლო

		მოთხოვნების, მგრძნობიარობისა და კრიტიკულობის გათვალისწინებით.
ა 7.2.2	ინფორმაციის მარკირება და მისი მოპყრობა	*კონტროლის მექანიზმი:* ჩამოყალიბდეს და დაინერგოს ინფორმაციის მარკირებისა და მისი მოპყრობის სათანადო პროცედურები ორგანიზაციაში მიღებული კლასიფიკაციის სქემის შესაბამისად.
ა.8 ადამიანური რესურსების უსაფრთხოება		
ა.8.1 დასაქმებამდე *მიზანი:* მომუშავე პერსონალის, კონტრაქტორების და მესამე მხარეების მიერ პასუხისმგებლობის გაცნობიერება, რათა მოხდეს დამუშავების საშუალებათა ქურდობის, თაღლითობის ან არამიზნობრივად გამოყენების თავიდან აცილება.		
ა 8.1.1	როლები და პასუხისმგებლობა	*კონტროლის მექანიზმი:* თანამშრომელთა, კონტრაქტორთა და მესამე მხარეთა როლები და პასუხისმგებლობა უნდა იყოს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისად განსაზღვრული და დოკუმენტირებული.
ა 8.1.2	გადამოწმება	*კონტროლის მექანიზმი:* უნდა განხორციელდეს დასაქმების კანდიდატების, კონტრაქტორების ან მესამე მხარეების შემოწმება კანონის, მარეგულირებლის და ეთიკის, ბიზნესის მოთხოვნების, სავარაუდო წვდომადი ინფორმაციის კლასიფიკაციის და სავარაუდო რისკების შესაბამისად,
ა 8.1.3	დასაქმების პირობები	*კონტროლის მექანიზმი:* დასაქმებულები, კონტრაქტორები და მესამე მხარეები ვალდებულნი არიან დაეთანხმონ და ხელი მოაწერონ დასაქმების კონტრაქტს, რომლის ფარგლებშიც იქნება განსაზღვრული მათი პასუხისმგებლობა ინფორმაციულ უსაფრთხოებაზე.
ა.8.2 დასაქმების პერიოდში *მიზანი*: დასაქმებულის, კონტრაქტორისა და მესამე მხარის შეტყობინება ინფორმაციული უსაფრთხოების საფრთხეების, მათი მოვალეობების და ვალდებულებების შესახებ, მათი უზრუნველყოფა აპარატურით, რათა მოხდეს ორგანიზაციული უსაფრთხოების პოლიტიკის მხარდაჭერა საქმიანობის დროს და შემცირდეს ადამიანური შეცდომის რისკი		

ა 8.2.1	მენეჯმენტის პასუხისმგებლობა	*კონტროლის მექანიზმი:* მენეჯმენტმა უნდა მოსთხოვოს თანამშრომლებს, კონტრაქტორებს და მესამე მხარეებს გამოიყენონ უსაფრთხოების ზომები ორგანიზაციაში არსებული უსაფრთხოების პოლიტიკების და პროცედურების შესაბამისად.
ა 8.2.2	ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლება, სწავლება და ტრენინგი	*კონტროლის მექანიზმი:* ორგანიზაციის ყველა თანამშრომელმა, და საჭიროების შემთხვევაში, კონტრაქტორებმა და მესამე მხარეებმა უნდა მიიღონ სათანადო ცნობიერების ამაღლების შესახებ ტრენინგი და ინფორმირებული იყვნენ ორგანიზაციული პოლიტიკების და პროცედურების განახლებების შესახებ, საქმიანობის შესრულების შესაბამისად.
ა 8.2.3	დისციპლინა	*კონტროლის მექანიზმი:* უნდა არსებობდეს გარკვეული დისციპლინარული პროცესი იმ თანამშრომლებისთვის, რომლებმაც საფრთხე შეუქმნეს ორგანიზაციის უსაფრთხოებას.
ა.8.3 სამსახურის შეცვლა ან გათავისუფლება *მიზანი:* თანამშრომლების, კონტრაქტორების და მესამე მხარეების ორგანიზაციიდან გასვლის, ან სამსახურებრივი პოზიციის შეცვლის წესების შესრულება		
ა 8.3.1	უფლებამოსილების შეწყვეტა	*კონტროლის მექანიზმი:* დასაქმების შეწყვეტის ან პოზიციის ცვლილების პასუხისმგებლობები უნდა იყოს ცალსახად განსაზღვრული და განაწილებული
ა 8.3.2	აქტივების დაბრუნება	*კონტროლის მექანიზმი:* ყველა დასაქმებული, კონტრაქტორი და მესამე მხარე დასაქმების შეწყვეტის შედეგად ვალდებულია დააბრუნოს მათ დაქვემდებარებაში არსებული ორგანიზაციის ყველა აქტივი.
ა 8.3.3	წვდომის უფლებების გაუქმება	*კონტროლის მექანიზმი:* თანამშრომელთა, კონტრაქტორთა და მესამე მხარეთა ინფორმაციაზე და ინფორმაციის დამუშავების საშუალებებზე წვდომის უფლებები უნდა გაუქმდეს საქმიანობის, კონტრაქტის ან შეთანხმების დასრულებასთან ერთად.
ა.9 ფიზიკური და გარემოს უსაფრთხოება		
ა.9.1 არეების დაცვა *მიზანი:* ორგაანიზაციის ინფორმაციაზე უნებართვო ფიზიკური წვდომის ან დაზიანების თავიდან აცილება.		

ა 9.1.1	ფიზიკური უსაფრთხოების პერიმეტრი	*კონტროლის მექანიზმი:* უსაფრთხოების პერიმეტრებში (ბარიერები, ისეთი როგორც კედლები, საბარათე კონტროლირებადი შესასვლელები, ან მისაღები ოთახები) ხდება ისეთი არეების დაცვა, სადაც განთავსებულია ინფორმაცია ან ინფორმაციის დამუშავების საშუალებები.
ა 9.1.2	ფიზიკური დაშვების კონტროლის მექანიზმები	*კონტროლის მექანიზმი:* დაცული არეების წვდომა უნდა იყოს შეზღუდული შესვლის კონტროლის შესაბამისი მექანიზმებით, რათა მხოლოდ ნებადართული პერსონალისთვის იყოს წვდომა შესაძლებელი.
ა 9.1.3	ოფისების, ოთახების და დამუშავების საშუალებების დაცვა	*კონტროლის მექანიზმი:* საჭიროა ოფისების, ოთახების და დამუშავების საშუალებების ფიზიკური დაცვის დაგეგმვა და გამოყენება.
ა 9.1.4	გარე და გარემოებრივი საფრთხეებისგან დაცვა	*კონტროლის მექანიზმი:* ხანძრის, დატბორვის, მიწისძვრის, აფეთქების, სამოქალაქო დაუმორჩილებლობის და სხვა ფორმის ბუნებრივი ან ადამიანური ფაქტორით გამოწვეული კატასტროფების საწინააღმდეგოდ უნდა დაიგეგმოს და დაინერგოს ფიზიკური უსაფრთხოება.
ა 9.1.5	დაცულ არეებში საქმიანობა	*კონტროლის მექანიზმი:* უდნა შეიქმნას და დაინერგოს ფიზიკური დაცვა და დაცულ არეებში მუშაობის სახელმძღვანელო მითითებები.
ა 9.1.6	საჯარო წვდომის, და მიღების/ჩატვირთვის არეები	*კონტროლის მექანიზმები:* საქონლის მიღების ან დაცლა/დატვირთვის არეებზე, სადაც შესაძლოა ადამიანების უნებართვო ყოფნა, უნდა განხორციელდეს კონტროლი, და თუ შესაძლებელია, ეს არეები იზოლირებული უნდა იყოს ინფორმაციის დამუშავების საშუალებებისგან, რათა არ მოხდეს მათზე უნებართვო წვდომა.
ა.9.2 მოწყობილობათა უსაფრთხოება *მიზანი:* ორგანიზაციის საქმიანობაში წყვეტის, აქტივების დაკარგვის, გაფუჭების ან მოპარვის თავიდან აცილება.		
ა 9.2.1	მოწყობილობათა განლაგება და დაცვა	*კონტროლის მექანიზმი:* მოწყობილობები განლაგებული ან დაცული უნდა იყოს გარემოს საფრთხეებისგან და უნებართვო წვდომისგან, რისკების შემცირების მიზნით.

ა 9.2.2	დამხმარე მოწყობილობები	*კონტროლის მექანიზმი:* დამუშავების საშუალებები დაცული უნდა იყოს ძაბვის ვარდნებისგან და სხვა გამანადგურებელი პროცესებისგან, რომელიც გამოწვეულია დამხმარე მოწყობილობებით.
ა 9.2.3	გაყვანილობის უსაფრთხოება	*კონტროლის მექანიზმი:* მონაცემთა დამუშავების დენის და საკომუნიკაციო გაყვანილობა უნდა იყოს დაცული ინფორმაციის მოპარვისა ან დაზიანებისგან.
ა 9.2.4	მოწყობილობათა მხარდაჭერა	*კონტროლის მექანიზმი:* უნდა მოხდეს მოწყობილობების მხარდაჭერა, რათა უზრუნველყოფილი იყოს მათი მუდმივი ხელმისაწვდომობა და სისრულე.
ა 9.2.5	ტერიტორიის გარეთ მყოფი მოწყობილობები	*კონტროლის მექანიზმი:* ტერიტორიის გარეთ მყოფ მოწყობილობებზე უნდა ვრცელდებოდეს დაცვა ტერიტორიის გარეთ საქმიანობის სხვადასხვა რისკის გათვალისწინებით.
ა 9.2.6	მოწყობილობათა უსაფრთხო განადგურება ან შემდგომი გამოყენება	*კონტროლის მექანიზმი:* განადგურებამდე ან ხელახლა გამოყენებამდე ყველა მოწყობილობის შემოწმება, არის თუ არა მასზე განთავსებული სენსიტიური ინფორმაცია და ლიცენზირებული პროგრამული უზრუნველყოფა წაშლილი.
ა 9.2.7	საკუთრების ამოღება	*კონტროლის მექანიზმი:* მოწყობილობები, ინფორმაცია ან პროგრამული უზრუნველყოფა არ უნდა გავიდეს ტერიტორიის გარეთ ნებართვის გარეშე.
ა.10 საკომუნიკაციო და საოპერაციო მართვა		
ა.10.1 საოპერაციო პროცედურები და პასუხისმგებლობები *მიზანი:* ინფორმაციის დამუშავების მოწყობილობების სწორი და უსაფრთხო მუშაობის უზრუნველყოფა		
ა 10.1.1	დოკუმენტირებული საოპერაციო პროცედურები	*კონტროლის მექანიზმი:* საოპერაციო პროცედურები უნდა იყოს დოკუმენტირებული და ხელმისაწვდომი ყველა მომხმარებლისთვის.
ა 10.1.2	ცვლილებათა მართვა	*კონტროლის მექანიზმი:* ინფორმაციის დამუშავების საშუალებების და სისტემების ცვლილებაზე უნდა ხორციელდებოდეს კონტროლი.

ა 10.1.3	მოვალეობათა განაწილება	*კონტროლის მექანიზმი:* მოვალეობები და პასუხისმგებლობის არეები უნდა იყოს გამიჯნული ორგანიზაციის აქტივების უნებართვო ან არაგანზრახ ცვლილების და ბოროტად გამოყენების თავიდან აცილების მიზნით.
ა 10.1.4	პროგრამული უზრუნველყოფის შემუშავების, სატესტო და საოპერაციო გარემოს გამიჯვნა	*კონტროლის მექანიზმი:* პროგრამული უზრუნველყოფის შემუშავების, ტესტირების და საოპერაციო გარემო უნდა იყოს გამიჯნული უნებართვო წვდომის ან ცვლილებების რისკების შემცირების მიზნით.
ა.10.2 მესამე მხარის მიერ მოწოდებული მომსახურების მართვა *მიზანი:* შემუშავდეს და შენარჩუნდეს ინფორმაციული უსაფრთხოების და მომსახურების მოწოდების სათანადო დონეები მომსახურების მოწოდების შესახებ შეთანხმებების შესაბამისად.		
ა 10.2.1	მომსახურების მოწოდება	*კონტროლის მექანიზმი:* მომწოდებლის შეთანხმებაში არსებული უსაფრთხოების კონტროლის მექანიზმები უნდა დაინერგოს, მომსახურების ჩამონათვალი და მომსახურების მოწოდების დონეების მართვა უნდა ხდებოდეს მესამე მხარის მიერ.
ა 10.2.2	მესამე მხარის მიერ მოწოდებული მომსახურების მონიტორინგი და განხილვა.	*კონტროლის მექანიზმი:* უნდა ხდებოდეს მესამე მხარის მიერ მოწოდებული მომსახურების, ანგარიშების და ჩანაწერების რეგულარული მონიტორინგი და განხილვა, აგრეთვე მათი აუდიტი.
ა 10.2.3	მესამე მხარის მიერ მოწოდებული მომსახურების ცვლილების მართვა	*კონტროლის მექანიზმი:* მომსახურების მოწოდების ცვილება, მათ შორის არსებული ინფორმაციული უსაფრთხოების პოლიტიკის, პროცედურის ან კონტროლის მექანიზმის შენარჩუნება და გაუმჯობესება, უნდა იმართებოდეს ბიზნეს სისტემების კრიტიკულობის, გამოყენებული პროცესების და რისკების გადაფასების გათვალისწინებით.
ა.10.3 სისტემის დაგეგმვა და მიღება *მიზანი:* სისტემების ჩავარდნის რისკის შემცირება		
ა 10.3.1	სისტემის სიმძლავრეების მართვა	*კონტროლის მექანიზმი:* რესურსების გამოყენების მონიტორინგი, გაუმჯობესება და მომავალი სიმძლავრეებისადმი მოთხოვნების პროგნოზირება უნდა კეთდებოდეს სისტემის არსებითი ფუნქციების შესასრულებლად.

ა 10.3.2	სისტემის მიღება	*კონტროლის მექანიზმი:* ახალი საინფორმაციო სისტემის, სისტემის გაუმჯობესების და ახალი ვერსიების მიღების კრიტერიუმები უნდა ჩამოყალიბდეს, აგრეთვე უნდა ჩატარდეს სისტემის დამუშავების დროს და მის ჩაბარებამდე შესაბამისი ტესტირება.
ა.10.4 მავნე და მობილური კოდისგან დაცვა *მიზანი:* პროგრამული უზრუნველყოფის და ინფომაციის მთლიანობის დაცვა		
ა 10.4.1	მავნე კოდის საწინააღმდეგო კონტროლის მექანიზმები	*კონტროლის მექანიზმი:* მავნე კოდისგან დაცვის მიზნით საჭიროა დაინერგოს აღმოჩენის, პრევენციული და აღდგენის კონტროლის მექანიზმები, აგრეთვე მომხმარებლის ცნობიერების ამაღლების პროცედურები.
ა 10.4.2	მობილური კოდის საწინააღმდეგო კონტროლის მექანიზმები	*კონტროლის მექანიზმი:* იქ, სადაც მობილური კოდის გამოყენება ნებადართულია, კონფიგურაციამ უნდა უზრუნველყოს განსაზღვრულ პოლიტიკასთან მობილური კოდის ცალსახა შესაბამისობაში მუშაობა, და არაავტორიზებული კოდის მუშაობის აკრძალვა.
ა.10.5 სარეზერვო ასლები *მიზანი*: ინფორმაციის და ინფორმაციის დამუშავების მოწყობილობების მთლიანობის და ხელმისაწვდომობის მხარდაჭერა		
ა 10.5.1	ინფორმაციის სარეზერვო ასლები	*კონტროლის მექანიზმი:* ინფორმაციის და პროგრამული უზრულველყოფის სარეზერვო ასლები პერიოდულად უნდა მოწმდებოდეს ორგანიზაციაში დანერგილი პოლიტიკის შესაბამისად.
ა.10.6 ქსელის უსაფრთხოების მართვა *მიზანი*: ქსელური ინფორმაციის და დამხმარე ინფრასტრუქტურის დაცვა		
ა 10.6.1	ქსელის კონტროლის მექანიზმები	*კონტროლის მექანიზმი:* ქსელის მართვა და კონტროლი უნდა ხორციელდებოდეს ადექვატურად, რათა უზრუნველყოფილი იყოს საფრთხეებისგან დაცვა ქსელში ჩართული სისტემებისა და პროგრამებისთვის, მათ შორის გადაცემის პროცესში მყოფი ინფორმაციისათვის.

ა 10.6.2	ქსელური მომსახურების უსაფრთხოება	*კონტროლის მექანიზმი:* ყველა ქსელური მომსახურების უსაფრთხოების ზომები, მომსახურების დონეები და მენეჯმენტის მოთხოვნები უნდა დადგინდეს და გათვალისწინებული იქნეს ქსელის მომსახურების შესახებ არსებულ შეთანხმებებში, მიუხედავად იმისა, ეს მომსახურება შიდაა თუ გარე.
ა.10.7 მედია-მატარებელების მართვა *მიზანი:* აქტივების უნებართვო გამჟღავნება, შეცვლა, ამოღება ან განადგურება, აგრეთვე ბიზნესის საქმიანობის შეწყვეტის თავიდან აცილება		
ა 10.7.1	გადაადგილებადი მედია-მატარებლების მართვა	*კონტროლის მექანიზმი:* უნდა ჩამოყალიბდეს გადაადგილებადი მედია-მატარებლების მართვის პროცედურები.
ა 10.7.2	მედია-მატარებლების განადგურება	*კონტროლის მექანიზმი:* ფორმალიზებული პროცედურის შესაბამისად უნდა მოხდეს მედია-მატარებლების უსაფრთხო განადგურება
ა 10.7.3	ინფორმაციის მოპყრობის პროცედურები	*კონტროლის მექანიზმი:* ინფორმაციის მოპყრობის და შენახვის პროცედურები უნდა ჩამოყალიბდეს, რათა ეს ინფორმაცია უნებართვო გამჟღავნებისგან ან გამოყენებისგან იყოს დაცული.
ა 10.7.4	სისტემის დოკუმენტაციის უსაფრთხოება	*კონტროლის მექანიზმი:* სისტემის დოკუმენტაცია უნდა იყოს დაცული არაავტორიზებული წვდომისაგან.
ა.10.8 ინფორმაციის გაცვლა *მიზანი:* ინფორმაციის და პროგრამული უზრუნველყოფის უსაფრთხოების შენარჩუნება ორგანიზაციის შიგნით ან სხვა გარე მხარესთან გაცვლისას.		
ა 10.8.1	ინფორმაციის გაცვლის პოლიტიკები და პროცედურები	*კონტროლის მექანიზმი:* ინფორმაციის უსაფრთხო გაცვლა ნებისმიერი საკომუნიკაციო საშუალებით უზრუნველყოფილი უნდა იყოს ფორმალური გაცვლის პოლიტიკებით, პროცედურებითა და კონტროლის მექანიზმებით.
ა 10.8.2	ინფორმაციის გაცვლის შესახებ შეთანხმებები	*კონტროლის მექანიზმი:* ინფორმაციის და პროგრამული უზრუნველყოფის გაცვლის შესახებ შეთანხმებები უნდა გაფორმდეს ორგანიზაციასა და გარე მხარეებს შორის.
ა 10.8.3	ფიზიკური მედია-მატარებლის გადაადგილება	*კონტროლის მექანიზმი:* ინფორმაციის მედია-მატარებელი უნდა იყოს დაცული არაავტორიზებული წვდომისაგან,

		გამოყენებისგან ან განადგურებისგან ორგანიზაციის ფარგლებს გარეთ გადაადგილების პროცესში.
ა 10.8.4	ელექტრონული მიმოწერა	*კონტროლის მექანიზმი:* ელექტრონულ მიმოწერაში მოხვედრილი ინფორმაცია უნდა იყოს სათანადოდ დაცული.
ა 10.8.5	ბიზნესის საინფორმაციო სისტემები	*კონტროლის მექანიზმი:* უნდა განისაზღვროს და დაინერგოს ბიზნესის საინფორმაცო სისტემების ურთიერთკავშირიდან გამომდინარე ინფორმაციის დაცვის პოლიტიკები და პროცედურები
ა.10.9 ელექტრონული კომერცია *მიზანი:* ელექტრონული კომერციის უსაფრთხოება და გამოყენება		
ა 10.9.1	ელექტრონული კომერცია	*კონტროლის მექანიზმი:* საჯარო ქსელებში მოძრავი ინფორმაცია ელექრტონული კომერციის შესახებ უნდა იყოს დაცული თაღლითობისგან, კონტრაქტის პირობების უგულებელყოფისგან და არაავტორიზებული გამჟღავნებისა და ცვლილებისგან.
ა 10.9.2	ონლაინ-ტრანზაქციები	*კონტროლის მექანიზმი:* ონლაინ-ტრანზაქციებში მონაწილე ინფორმაცია უნდა იყოს დაცული გადაგზავნის პროცესში წყვეტისგან, არასწორი გადაგზავნისგან, შეტყობინების არაავტორიზებული ცვლილებისგან, გამჟღავნებისგან, დუბლირებისგან ან ხელმეორედ გადაგზავნისაგან.
ა 10.9.3	საჯაროდ ხელმისაწმდომი ინფორმაცია	*კონტროლის მექანიზმი:* საჯაროდ ხელმისაწვდომი ან საჯარო სისტემაში არსებული ინფორმაციის მთლიანობა უნდა იყოს დაცული არაავტორიზებული ცვლილებისგან.
ა.10.10 მონიტორინგი *მიზანი*: ინფორმაციის არაავტორიზებული დამუშავების აღმოჩენა		
ა 10.10.1	აუდიტის შესახებ ჩანაწერები	*კონტროლის მექანიზმი:* მომხმარებლის მოქმედებები, გამონაკლისები, ინფორმაციის უსაფრთხოების მოვლენების შესახებ უნდა ხდებოდეს ჩანაწერების წარმოება და ინახებოდეს განსაზღვრული დროით, რათა დაეხმაროს მომავალ გამოძიებებში და წვდომის ზედამხედველობის კონტროლში.

ა 10.10.2	სისტემის გამოყენების მონიტორინგი	*კონტროლის მექანიზმი:* ინფორმაციის დამუშავების მოწყობილობების გამოყენების მონიტორინგის პროცედურები უნდა ჩამოყალიბდეს და მისი შედეგები გადაიხედოს პერიოდულად.
ა 10.10.3	ლოგირების ჩანაწერების დაცვა	*კონტროლის მექანიზმი:* ლოგირების მოწყობილობები და ლოგირების ჩანაწერები უდნა იყოს დაცული ცვლილებისგან და არაავტორიზებული წვდომისგან.
ა 10.10.4	ადმინისტრატორის და ოპერატორის ლოგები	*კონტროლის მექანიზმი:* უნდა ხდებოდეს სისტემის ადმინისტრატორის და სისტემის ოპერატორის მოქმედებათა ლოგირება.
ა 10.10.5	შეცდომების ლოგები	*კონტროლის მექანიზმი:* უნდა მოხდეს შეცდომების ლოგირება, მათი შესწავლა და განხორციელდეს შესაბამისი მოქმედება.
ა 10.10.6	საათის სინქრონიზაცია	*კონტროლის მექანიზმი:* ორგანიზაციის ან უსაფრთხოების ზონის ფარგლებში არსებული ინფორმაციული სისტემების საათი უნდა სინქრონიზირდებოდეს შეთანხმებულ სანდო დროის წყაროსთან.
ა.11 წვდომის კონტროლი		
ა.11.1 წვდომის კონტროლისთვის ბიზნეს მოთხოვნები *მიზანი:* ინფორმაციაზე წვდომის კონტროლი		
ა 11.1.1	წვდომის კონტროლის პოლიტიკა	*კონტროლის მექანიზმი:* წვდომის კონტროლის პოლიტიკა უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და გადაიხედოს ბიზნესის და უსაფრთხოების მოთხოვნებიდან გამომდინარე.
ა.11.2 მომხმარებელთა წვდომის მართვა *მიზანი:* ინფორმაციულ სისტემაში მომხმარებელთა ნებადართული წვდომის უზრუნველყოფა და არაავტორიზებული წვდომის თავიდან აცილება		
ა 11.2.1	მომხმარებელთა რეგისტრაცია	*კონტროლის მექანიზმი:* ინფორმაციულ სისტემაში მომხმარებლების დასაშვებად უნდა არსებობდეს ფორმალური რეგისტრაციისა და რეგისტრაცის გავლაზე უარის პროცედურა.
ა 11.2.2	პრივილეგიების მართვა	*კონტროლის მექანიზმი:* პრივილეგიების მინიჭება და მათი გამოყენება უნდა იყოს შეზღუდული და მართვადი.

ა 11.2.3	მომხმარებელთა პაროლების მართვა	*კონტროლის მექანიზმი:* პაროლების გაცემა უნდა იმართებოდეს მართვის ფორმალური პროცესის მიერ.
ა 11.2.4	მომხმარებელთა წვდომის უფლებების მიმოხილვა	*კონტროლის მექანიზმი:* მენეჯმენტმა პერიოდულად უნდა განიხილოს მომხმარებელთა წვდომის უფლებები.
ა.11.3 მომხმარებელთა პასუხისმგებლობები *მიზანი:* ინფორმაციაზე და ინფორმაციის დამუშავების მოწყობილობებზე არაავტორიზებული წვდომის, მათი უკანონო მითვისების და საფრთხის ქვეშ დაყენების თავიდან არიდება		
ა 11.3.1	პაროლების გამოყენება	*კონტროლის მექანიზმი:* მომხმარებელი ვალდებულია პაროლების შერჩევა და გამოყენება განახორციელოს არსებული საუკეთესო პრაქტიკების მიხედვით.
ა 11.3.2	უყურადღებოდ დატოვებული მოწყობილობები	*კონტროლის მექანიზმი:* მომხმარებლებმა უნდა უზრუნველყონ უმეთვალყურეოდ დარჩენილი მოწყობილობების სათანადოდდაცვა.
ა 11.3.3	„სუფთა მაგიდა და სუფთა ეკრანის“ პოლიტიკა	*კონტროლის მექანიზმი:* ნაბეჭდი მასალებისა და გადააადგილებადი მედია-მატარებლებისათვის უნდა გამოიყენებოდეს სუფთა მაგიდის პოლიტიკა, ინფორმაციის დამუშავების საშუალებებისათვის კი - სუფთა ეკრანის პოლიტიკა.
ა.11.4 ქსელური წვდომის კონტროლი *მიზანი:* ქსელურ სერვისებზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.4.1	ქსელური სერვისების გამოყენების პოლიტიკა	*კონტროლის მექანიზმი:* მომხმარებლებს უნდა მიეცეთ წვდომა მხოლოდ იმ რესურსებზე, რომლებზეც მათ გააჩნიათ ავტორიზებული უფლება.
ა 11.4.2	გარე კავშირისთვის მომხმარებელთა აუტენტიფიკაცია	*კონტროლის მექანიზმი:* სათანადო აუტენტიფიკაციის მეთოდები უნდა გამოიყენებოდეს დისტანციური მომხმარებლების მიერ წვდომის გასაკონტროლებლად.
ა 11.4.3	ქსელში არსებული მოწყობილობების იდენტიფიცირება	*კონტროლის მექანიზმი:* სხვადასხვა ადგილიდან ქსელური მოწყობილობების მიერთების აუტენტიფიკაციის მექანიზმი უნდა იყოს მოწყობილობათა ავტომატური იდენტიფიკაციის საშუალება.
ა 11.4.4	დაშორებული დიაგნოსტიკა და საკონფიგურაციო პორტების დაცვა	*კონტროლის მექანიზმი:*

		დიაგნოსტიკური და საკონფიგურაციო პორტების ფიზიკურ და ლოგიკურ წვდომაზე უნდა ხორციელდებოდეს კონტროლი.
ა 11.4.5	განცალკევება ქსელებში	*კონტროლის მექანიზმი:* ინფორმაციულ მომსახურებათა, მომხმარებელთა და საინფორმაციო სისტემათა ჯგუფები უნდა იყოს ქსელში განცალკევებული
ა 11.4.6	ქსელთან მიერთების კონტროლი	*კონტროლის მექანიზმი:* საერთო ქსელებისთვის, განსაკუთრებით რომლებიც ცდებიან ორგანიზაციის ფარგლებს, მომხმარებელთა ქსელთან მიერთების შესაძლებლობა უნდა იყოს შეზღუდული და იყოს წვდომის პოლიტიკის და ბიზნესის მხარდამჭერი სისტემების მოთხოვნებთან შესაბამისობაში.
ა 11.4.7	ქსელური მარშრუტიზაციის კონტროლი	*კონტროლის მექანიზმი:* ქსელების მარშრუტიზაციის კონტროლის მექანიზმები უნდა დაინერგოს ქსელებისთვის, რათა კომპიუტერის კავშირი და ინფორმაციის დინება დაცული იყოს გაჟონვისა და წვდომის პოლიტიკის დარღვევისგან.
ა.11.5 საოპერაციო სისტემაზე წვდომის კონტროლი *მიზანი:* საოპერაციო სისტემაზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.5.1	სისტემაში დაცული შესვლის პროცედურები	*კონტროლის მექანიზმი:* საოპერაციო სისტემებთან წვდომა უნდა ხდებოდეს შესვლის დაცული პროცედურის მიხედვით.
ა 11.5.2	მომხმარებელთა იდენტიფიკაცია და აუტენტიფიკაცია	*კონტროლის მექანიზმი:* ყველა მომხმარებელი უნდა ფლობდეს მხოლოდ მათი პერსონალური მოხმარებისთვის განკუთვნილ უნიკალურ იდენტიფიკატორს, და შესაბამისი აუტენტიფიკაციის მეთოდი უნდა იყოს არჩეული მომხმარებლის იდენტიფიკაციის საკმარისი მტკიცებულებისათვის.
ა 11.5.3	პაროლების მართვის სისტემა	*კონტროლის მექანიზმი:* პაროლების მართვის სისტემა უნდა იყოს ინტერაქტიული და უზრუნველყოფდეს ხარისხიან პაროლებს.
ა 11.5.4	დამხმარე სისტემური პროგრამების გამოყენება	*კონტროლის მექანიზმი:* სისტემის დამხმარე პროგრამების გამოყენება, რომლებსაც შეუძლიათ სისტემის შეზღუდვების და კონტროლების უგულებელყოფა, მკაცრად უნდა შეიზღუდოს და გაკონტროლდეს.

ა 11.5.5	სესიის ვადის ამოწურვა	*კონტროლის მექანიზმი:* არააქტიური სესიები უნდა დაიხუროს წინასწარ დადგენილი ვადის გასვლის შემდეგ.
ა 11.5.6	დაკავშირების ხანგრძლივობის შეზღუდვა	*კონტროლის მექანიზმი:* უნდა დადგინდეს დაკავშირების ხანგრძლივობის შეზღუდვა მაღალი რისკის შემცველი პროგრამული უზრუნველყოფის დამატებითი დაცვისათვის.
ა.11.6 პროგრამული უზრუნველყოფზე და ინფორმაციაზე წვდომის კონტროლი *მიზანი:* პროგრამულ უზრუნელყოფაში არსებულ ინფორმაციაზე არაავტორიზებული წვდომის თავიდან არიდება		
ა 11.6.1	ინფორმაციაზე წვდომის შეზღუდვა	*კონტროლის მექანიზმი:* მომხმარებელთა და დამხმარე პერსონალის წვდომა ინფორმაციაზე და იფნორმაციული სისტემების ფუნქციებზე უნდა იყოს შეზღუდული წვდომის პოლიტიკის შესაბამისად.
ა 11.6.2	სენსიტიური ინფორმაციის იზოლირება	*კონტროლის მექანიზმი:* სენსიტიურ სისტემებს უნდა გააჩნდეთ გამოყოფილი (იზოლირებული) გარემო.
ა.11.7 მობილური ტექნოლოგიები და დისტანციური მუშაობა *მიზანი:* ინფორმაციის უსაფრთხოების უზრუნველყოფა მობილური ტექნოლოგიებისა და და დისტანციური მუშაობის შემთხვევაში.		
ა 11.7.1	მობილური ტექნოლოგიების გამოყენება და კავშირგაბმულობა	*კონტროლის მექანიზმი:* პოლიტიკა უნდა ჩამოყალიბდეს და შესაბამისი უსაფრთხოების ზომები უნდა იქნეს მიღებული მობილური ტექნოლოგიების და კავშირგაბმულობის გამოყენებისას რისკებისგან თავის დასაცავად.
ა 11.7.2	დისტანციური მუშაობა	*კონტროლის მექანიზმი:* პოლიტიკა, საოპერაციო გეგმა და პროცედურები უნდა შემუშავდეს და დაინერგოს დისტანციური მუშაობის შემთხვევაში.
ა.12 ინფორმაციული სისტემების შეძენა, დამუშავება და შენარჩუნება		
ა.12.1 ინფორმაციული სისტემების უსაფრთხოების მოთხოვნები *მიზანი:* უზრუნველყოფილი უნდა იყოს უსაფრთხოება, როგორც ინფორმაციული სისტემის განუყოფელი ნაწილი		
ა 12.1.1	უსაფრთხოების მოთხოვნების ანალიზი და მახასიათებლები	*კონტროლის მექანიზმი:* უსაფრთხოების კონტროლის მოთხოვნები უნდა იყოს ახალი სისტემის ან არსებული სისტემის გაუმჯობესებისთვის საჭირო ბიზნეს-მოთხოვნების ნაწილი

ა.12.2 პროგრამული უზრუნველყოფის სწორი დამუშავება *მიზანი:* პროგრამულ უზრუნველყოფაში არსებული ინფორმაციის შეცდომების, დაკარგვის, არაავტორიზებული ცვლილებისა და გამოყენებისგან დაცვა		
ა 12.2.1	შემავალი მონაცემების შემოწმება	*კონტროლის მექანიზმი:* პროგრამულ უზრუნველყოფაში შემავალი ინფორმაცია უნდა მოწმდებოდეს სისწორეზე და შესაბამისობაზე.
ა 12.2.2	შიდა დამუშავების კონტროლი	*კონტროლის მექანიზმი:* პროგრამულ უზრუნველყოფას უნდა გააჩნდეს შემოწმების საშუალებები, რათა აღმოჩენილ იქნეს ინფორმაციის ნებისმიერი დაზიანება დამუშავების პროცესში ან განზრახ ქმედების შედეგად.
ა 12.2.3	შეტყობინების მთლიანობა	*კონტროლის მექანიზმი:* პროგრამულ უზრუნველყოფაში უნდა დაინერგოს შეტყობინების აუტენტურობის და მთლიანობის დამცავი მოთხოვნები, ასევე გამოვლინდეს და დაინერგოს შესაბამისი კონტროლის მექანიზმები
ა 12.2.4	გამომავალი ინფორმაციის შემოწმება	*კონტროლის მექანიზმი:* პროგრამული უზრუნველყოფის გამომავალი ინფორმაცია უნდა მოწმდებოდეს არსებული ინფორმაციის დამუშავების სისწორეზე და შესაბამისობაზე.
ა.12.3 კრიპტოგრაფიული კონტროლის მექანიზმები *მიზანი:* ინფორმაციის კონფიდენციალურობის, აუტენტურობის და მთლიანობის დაცვა კრიპტოგრაფიული საშუალებებით.		
ა. 12.3.1	კრიპტოგრაფიული მეთოდების გამოყენების პოლიტიკა	*კონტროლის მექანიზმი:* ინფორმაციის დაცვის კრიპტოგრაფიული მეთოდების გამოყენების პოლიტიკა უნდა ჩამოყალიბდეს და დაინერგოს.
ა 12.3.2	გასაღებების მართვა	*კონტროლის მექანიზმი:* ორგანიზაციაში კრიპტოგრაფიული ხერხების გამოყენების მიზნით უნდა არსებობდეს გასაღებების მართვის პროცესი.
ა.12.4 სისტემური ფაილების უსაფრთხოება *მიზანი:* სისტემური ფაილების უსაფრთხოების უზრუნველყოფა		
ა 12.4.1	საოპერაციო სისტემების კონტროლი	*კონტროლის მექანიზმი:* საოპერაციო სისტემებზე პროგრამების ინსტალაცია

		უნდა კონტროლდებოდეს შესაბამისი პროცედურის მიერ.
ა 12 4.2	სისტემის სატესტო მონაცემების დაცვა	*კონტროლის მექანიზმი:* სატესტო მონაცემების შერჩევა უნდა მოხდეს ყურადღებით, იყოს დაცული და კონტროლდებოდეს.
ა 12.4.3	პროგრამის კოდზე წვდომის კონტროლი	*კონტროლის მექანიზმი:* პროგრამის კოდზე წვდომა უნდა იყოს შეზღუდული.
ა.12.5 უსაფრთხოება დამუშავებასა და მხარდამჭერ პროცესებში *მიზანი:* პროგრამული სისტემის და ინფორმაციის უსაფრთხოების შენარჩუნება		
ა 12.5.1	ცვლილების კონტროლის პროცედურები	*კონტროლის მექანიზმი:* ცვლილებების დანერგვა უნდა კონტროლდებოდეს ცვლილების კონტროლის პროცედურების მიხედვით.
ა 12.5.2	საოპერაციო სისტემის ცვლილებების შემდგომი პროგრამული უზრუნველყოფის ტექნიკური მიმოხილვა	*კონტროლის მექანიზმი:* იმ შემთხვევაში, როდესაც ხდება საოპერაციო სისტემის ცვლილება, უნდა მოხდეს ბიზნესის კრიტიკული პროგრამული უზრუნველყოფის განხილვა და ტესტირება ორგანიზაციის ოპერაციებზე და უსაფრთხოებაზე უარყოფითი გავლენის თავიდან ასაცილებლად.
ა 12.5.3	პროგრამული პაკეტების ცვლილებების შეზღუდვა	*კონტროლის მექანიზმი:* პროგრამული პაკეტების ცვლილებები უნდა განხორციელდეს მხოლოდ აუცილებელობის შემთხვევაში და უნდა კონტროლდებოდეს მკაცრად.
ა 12.5.4	ინფორმაციის გაჟონვა	*კონტროლის მექანიზმი:* ინფორმაციის შესაძლო გაჟონა უნდა იქნეს თავიდან არიდებული.
ა 12.5.5	პროგრამის შექმნა/დამუშავება მესამე მხარის მიერ.	*კონტროლის მექანიზმი:* უნდა ხდებოდეს მესამე მხარის მიერ შექმნილი/დამუშავებული პროგრამების ზედამხედველობა და ორგანიზაციის მიერ მათზე მონიტორინგის განხორციელება.
ა.12.6 ტექნიკური სისუტეების მართვა *მიზანი:* ცნობილი ტენიკური სისუსტეებით სარგებლობისგან გამოწვეული რისკის შემცირება		
ა 12.6.1	ტექნიკური სისუსტეების მართვა	*კონტროლის მექანიზმი:* ინფორმაციული სისტემების ტექნიკური სისუსტეების შესახებ მოძიებული უნდა იქნეს ოპერატიული ინფორმაცია, ორგანიზაციის ამ სისუსტეებისადმი დამოკიდებულება შეფასდეს, და

		შესაბამისი ზომები მიღებულ იქნეს არსებული რისკებზე რეაგირებისთვის.
ა.13 ინფორმაციული უსაფრთხოების ინციდენტების მართვა		
ა.13.1 ინფორმაციული უსაფრთხოების მოვლენების და სისუსტეების შესახებ ანგარიში *მიზანი:* ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მოვლენების და სისუსტეების შესახებ შეტყობინებები ხდება დროულად		
ა 13.1.1	ინფორმაციული უსაფრთხოების მოვლენების ანგარიში	*კონტროლის მექანიზმი:* ინფორმაციული უსაფრთხოების მოვლენების შესახებ ანგარიშგება ხდება ოპერატიულად შესაბამისი მართვის არხების მეშვეობით
ა 13.1.2	უსაფრთხოების სისუსტის ანგარიში	*კონტროლის მექანიზმი:* ინფორმაციული სისტემის და მომსახურების გამომყენებელი ყველა თანამშრომელი, კონტრაქტორი ან მესამე მხარის მომხმარებელი ვალდებულია აცნობოს შენიშნული ან სავარაუდო უსაფრთხოების სისუსტის შესახებ.
ა.13.2 ინფორმაციული უსაფრთხოების ინციდენტების და გაუჯობესებების მართვა *მიზანი:* უზრუნველყოფილი უნდა იყოს მუდმივი და ეფექტიანი მიდგომის გამოყენება ინფორმაციული უსაფრთხოების ინციდენტების მართვაში.		
ა 13.2.1	პასუხისმგებლობები და პროცედურები	*კონტროლის მექანიზმი:* უნდა განისაზღვროს მენეჯმენტის პასუხისმგებლობები და პროცედურები, რათა მოხდეს სწრაფი, ეფექტიანი და სათანადო რეაგირება ინფორმაციული უსაფრთხოების ინციდენტზე.
ა 13.2.2	ინფორმაციული უსაფრთხოების ინციდენტებიდან მიღებული ცოდნა	*კონტროლის მექანიზმი:* უნდა არსებობდეს მექანიზმი, რომლის მეშვეობითაც მოხდება ინფორმაციული უსაფრთხოების ინციდენტების აღრიცხვა და ზედამხედველობა მისი ტიპის, მოცულობის და ღირებულების მიხედვით.
ა 13.2.3	მტკიცებულებების მოძიება	*კონტროლის მექანიზმი:* უნდა მოხდეს მტკიცებულებების მოძიება, დაცვა და წარდგენა, როდესაც პიროვნების ან ორგანიზაციის წინააღმდეგ ხორციელდება სამოქალაქო ან სისხლის სამართლის წარმოება.
ა.14 ბიზნესის უწყვეტობის მართვა		
ა.14.1 ბიზნესის უწყვეტობის მართვის ინფორმაციული უსაფრთხოების ასპექტები. *მიზანი:* ბიზნესის წყვეტის წინააღმგედ და ბიზნესის კრიტიკული პროცესების დასაცავად მიმართული ქმედება, ინფორმაციული სისტემის მნიშვნელოვანი წარუმატებლობის/მარცხის ან სტიქიური უბედურების შემთხვევაში დროული აღდგენა.		
ა 14.1.1	ბიზნესის უწყვეტობის მართვის	*კონტროლის მექანიზმი:*

	პროცესში ინფორმაციული უსაფრთხების გათვალისწინება.	უნდა შემუშავდეს და შენარჩუნდეს ორგანიზაციის ბიზნესის უწყვეტობის პროცესი, რომელიც ივალისწინებს ინფორმაციული უსაფრთხოების მოთხოვნებს.
ა 14.1.2	ბიზნესის უწყვეტობა და რისკების შეფასება	*კონტროლის მექანიზმი:* გამოვლენილი უნდა იყოს ის მოვლენები, რომლებმაც შესაძლოა იმოქმედოს ბიზნეს-პროცესების წყვეტაზე, აგრეთვე ამ წყვეტის ალბათობა, ეფექტი და გავლენა ინფორმაციულ უსაფრთხოებაზე.
ა 14.1.3	ინფორმაციული უსაფრთხოების შემცველი ბიზნესის უწყვეტობის გეგმების შემუშავება	*კონტროლის მექანიზმი:* უნდა შემუშავდეს და დაინერგოს გეგმები, რომლებიც მოიცავს ოპერაციების შენარჩუნებას ან აღდგენას, ასევე სათანადო დონეზე და მისაღებ დროში ბიზნეს პროცესის წყვეტის ან გაჩერების შემდეგ უზრუნველყოფს ინფორმაციის ხელმისაწვდომობას.
ა 14.1.4	ბიზნესის უწყვეტობის დაგეგმარების სტრატეგია.	*კონტროლის მექანიზმი:* უნდა შემუშავდეს ბიზნესის უწყვეტობის ერთიანი დაგეგმარების სტრატეგია ყველა გეგმის თავსებადობაში მოსაყვანად, რომელიც თანმიმდევრულად პასუხობს ინფორმაციული უსაფრთხოების მოთხოვნებს, აღწერს ტესტირების და შენარჩუნების პრიორიტეტებს.
ა 14.1.5	ბიზნეს უწყვეტობის გეგმების ტესტირება, შენარჩუნება და ხელახლა შეფასება	*კონტროლის მექანიზმი:* უნდა ხდებოდეს ბიზნეს უწყვეტობის გეგმების რეგულარული ტესტირება და განახლება მათი თანამედროვეობის და ეფექტიანობის უზრუნველსაყოფად.
ა.15 შესაბამისობა		
ა.15.1 იურიდიულ მოთხოვნებთან შესაბამისობა *მიზანი:* ნებისმიერი იურიდიული, მარეგულირებელი და საკონტრაქტო ვალდებულებების და უსაფრთხოების მოთხოვნების დარღვევის თავის არიდება.		
ა 15.1.1	გამოსაყენებელი იურიდიული ბაზის დადგენა	*კონტროლის მექანიზმი:* ყველა მნიშვნელოვანი იურიდიული, მარეგულირებელი და საკონტრაქტო მოთხოვნა და ორგანიზაციის მიდგომა ამ მოთხოვნების დაკმაყოფილებისადმი უნდა განისაზღვროს ცალსახად და იყოს მოქმედი ყოველი საინფორმაციო სისტემისა და ორგანიზაციისთვის.

ა 15.1.2	ინტელექტუალური საკუთრების უფლებები	*კონტროლის მექანიზმი:* ინტელექტუალური საკუთრების ან კერძო პროგრამული პროდუქტის გამოყენების შემთხვევაში უნდა დაინერგოს შესაბამისი პროცედურა, რომელიც უზრუნველყოფს იურიდიულ, მარეგულირებელ და საკონტრაქტო მოთხოვნებთან შესაბამისობას.
ა 15.1.3	ორგანიზაციული ჩანაწერების დაცვა	*კონტროლის მექანიზმი:* მნიშვნელოვანი ორგანიზაციული ჩანაწერები უნდა იყოს დაცული დაკარგვისგან, განადგურებისგან და გაყალბებისგან კანონის მიერ დადგენილ, მარეგულირებელ, საკონტრაქტო და ბიზნეს-მოთხოვნებთან შესაბამისად.
ა 15.1.4	მონაცემთა დაცვა და პირადი ინფორმაციის საიდუმლოება	*კონტროლის მექანიზმი:* მონაცემთა დაცვა და საიდუმლოება უნდა იყოს უზრუნველყოფილი იურიდიული, მარეგულირებელი და, როდესაც სჭიროა, საკონტრაქტო ვალდებულებების შესაბამისად.
ა 15.1.5	ინფორმაციის დამუშავების საშუალებათა არამიზნობრივად გამოყენების აღკვეთა	*კონტროლის მექანიზმი:* ინფრომაციის დამუშავების საშუალებების არამიზნობრივად გამოყენება მომხმარებლების მიერ უნდა აღიკვეთოს.
ა 15.1.6	კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენების რეგულაცია	*კონტროლის მექანიზმი:* კრიპტოგრაფიული კონტროლის მექანიზმები უნდა გამოყენებოდეს იურიდიული, მარეგულირებელი და საკონტრაქტო მოთხოვნების შესაბამისად.
ა.15.2 უსაფრთხოების პოლიტიკებთან და სტანდარტებთან შესაბამისობა და ტექნიკური შესაბამისობა *მიზანი:* სისტემების შესაბამისობის უზრუნველყოფა ორგანიზაციის უსაფრთხოების პოლიტიკებსა და სტანდარტებთან		
ა 15.2.1	უსაფრთხოების პოლიტიკებსა და სტანდარტებთან შესაბამისობა.	*კონტროლის მექანიზმი:* მენეჯერებმა უნდა უზრუნველყონ საკუთარი პასუხისმგებლობის არეში მოქმედი ყველა უსაფრთხოების პროცედურის შესრულება უსაფრთხოების პოლიტიკებსა და სტანდარტებთან შესაბამისობის მისაღწევად.
ა 15.2.2	ტექნიკური შესაბამისობის შემოწმება	*კონტროლის მექანიზმი:* ინფორმაციული სისტემები მუდმივად უნდა მოწმდებოდეს უსაფრთხოების დანერგვის სტანდარტებთან შესაბამისობაზე.
ა.15.3 ინფორმაციული სისტემების აუდიტის რეკომენდაციები		

მიზანი: ინფორმაციული სისტემების აუდიტის პროცესის შედეგის ეფექტიანობის გაზრდა და მისი ჩარევის მინიმუმამდე დაყვანა.		
ა 15.3.1	ინფორმაციული სისტემების აუდიტის კონტროლები	*კონტროლის მექანიზმი:* საოპერაციო სისტემების აუდიტის მოთხოვნები და ქმედებები საგულდაგულოდ უნდა დაიგეგმოს და შეთანხმდეს ბიზნეს-პროცესის წყვეტის რისკის შესამცირებლად.
ა 15.3.2	ინფორმაციული სისტემების აუდიტის საშუალებების დაცვა.	*კონტროლის მექანიზმი:* ინფორმაციული სისტემების აუდიტის საშუალებების წვდომა უნდა იყოს დაცული არაავტორიზებული გამოყენებისა და კომპრომეტირებისგან.

მუხლი 3. გარდამავალი დებულება

1. საჯარო სამართლის იურიდიული პირი - კიბერუსაფრთხობის ბიურომ 2014 წლის 1 სექტემბრამდე შეიმუშაოს:

ა) თავდაცვის სფეროში კრიტიკული ინფორმაციული სუბიექტებისათვის აუცილებელი შესასრულებელი მოთხოვნები.

ბ) თავდაცვის სფეროში კრიტიკული ინფორმაციული ტექნოლოგიების უსაფრთხოების საშუალებების ინფორმაციული უსაფრთხოების მართვის სისტემები-მოთხოვნების შემუშავება.