ინფორმაციული უსაფრთხოების პოლიტიკა

ინფორმაცია დოკუმენტზე

ვერსია:	V5.0
ცვლილების თარიღი:	15.08.2024
პასუხისმგებელი პირი:	ინფორმაციული უსაფრთხოების მენეჯერი
კლასიფიკატორი:	საჯარო დოკუმენტი

ცვლილებების ისტორია

თარიღი:	ვერსია:	დოკუმენტის დამტკიცებაზე პასუხისმგებელი პირი	ცვლილებ(ებ)ის მოკლე აღწერა:
25.10.2021	V3.0	ლაშა გიორგი ჭელიძე	ცვლილებები ინფორმაციული უსაფრთხოების მიზნების და ამოცანების თაობაზე
27.04.2023	V4.0	ლაშა გიორგი ჭელიძე	შეიცვალა პუნქტი 12.3.2.1
12.03.2024		ლაშა გიორგი ჭელიძე	დოკუმენტის გადახედვა მოხდა ცვლილების გარეშე
15.08.2024	V 5.0	ლაშა გიორგი ჭელიძე	შეიცვალა 1.3; 2 მუხლი, 3.1,3.22,4.1.2 და 4.1.3, 4.2 პუქნტები, ამოღებულ იქნა მე- 7 მუხლი (სამუშაო ჯგუფი), შეიცვალა 10.3.2 და 10.3.3 პუნქტები, ასევე 13.3 პუნქტი, დაემატა 14 მუხლი, შეიცვალა 16-19 მუხლები.

სარჩევი

1. შესავალი 4
2. ტერმინთა განმარტება 4
3. მიზნები და ამოცანები 5
4. გავრცელების სფერო 6
5. ინფორმაციული უსაფრთხოების საბჭო 6
6. ინფორმაციული უსაფრთხოების მენეჯერი 7
7. მესამე მხარე 7
8. აქტივების მართვა 7
9. რისკების მართვა 7
10. კონტროლის მექანიზმების გამოყენებადობის განაცხადი 8
11. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა 8
12. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია 9
13. ინფორმაციული უსაფრთოხების ინციდენტების მართვა 9
14. ბიზნეს უწყვეტობის მართვა 9
15. კომუნიკაცია 9
16. იუმს-ის აუდიტი და უსაფრთხოების დონის შეფასება 10
18. მუდმივი გაუმჯობესება 10
19. პოლიტიკის გადახედვა 11

ინფორმაციული უსაფრთხოების პოლიტიკა

1. შესავალი

1.1. კომპანია იუჯითის მისიისა და მიზნების წარმატებით შესრულებისთვის, მნიშვნელოვანია ორგანიზაციის (კომპანიის) ბიზნეს პროცესებში ჩართული ინფორმაციული აქტივების უსაფრთხოების სათანადო დონის უზრუნველყოფა. ორგანიზაციაში არსებული ძირითადი ბიზნეს პროცესები დაკავშირებულია ინფორმაციის დამუშავება-შენახვასთან, როგორც ელექტრონული ასევე არაელექტრონული სახით, შესაბამისად მნიშვნელოვანია მათი სათანადო დონეზე დაცვა **(კონფიდენციალობა, ხელმისაწვდომობა** და **მთლიანობა)** ისეთი საფრთხეებისგან, როგორიც არის არასანქცირებული წვდომა, ინფორმაციის გაჟონვა ან დაკარგვა, ინფორმაციული ტექნოლოგიების სისტემების ან სერვისების შეფერხება/დაზიანება.

1.2. კომპანია იუჯითის ხელმძღვანელობა ამტკიცებს წინამდებარე ინფორმაციული უსაფრთხოების პოლიტიკას (შემდგომში - „პოლიტიკა“-ს):

1.2.1. კომპანიაში ინფორმაციული უსაფრთხოების დონის ასამაღლებლად;

1.2.2. ინფორმაციული უსაფრთხოების მართვის სისტემის დაგეგმარების, დანერგვის, ფუნქციონირების, მონიტორინგისა და მუდმივი გაუმჯობესების მიზნით.

1.3. ინფორმაციული უსაფრთხოების პოლიტიკა ეფუძნება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონს და ინფორმაციული უსაფრთხოების სტანდარტს ISO/IEC 27001;

1.4. პოლიტიკა შეიცავს ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანს, ძირითად მიმართულებას და პრინციპებს.

2. ტერმინთა განმარტება

პოლიტიკაში გამოყენებული ტერმინებს აქვთ შემდეგი განმარტებები:

2.1. **ინფორმაციული უსაფრთხოება** – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

2.2. **ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები** - საბაზისო მოთხოვნები, რომლებიც ორგანიზაციამ უნდა შეასრულოს თანმიმდევრულად უსაფრთხოების მართვის სისტემის დასანერგად;

2.3. **ინფორმაციული აქტივი** – ყველა ინფორმაცია და ცოდნა (მათ შორის, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია ორგანიზაციისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

2.4. **კონფიდენციალობა** - აქტივის მახასიათებელი, რომლის თანახმადაც აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის;

2.5. **მთლიანობა** - აქტივის სიზუსტის და სისრულის მახასიათებელი;

2.6. **ხელმისაწვდომობა** - ავტორიზებული სუბიექტის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი;

2.7. **ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომში - იუმს)** - მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

2.8. **რისკის ანალიზი** - რისკის წარმოშობის წყაროსა და რისკის დონის შეფასების პროცესი, რომლის საფუძველზეც ხდება რისკების შეფასება და რისკის მოპყრობის შესახებ გადაწყვეტილების მიღება. რისკის ანალიზი ასევე მოიცავს რისკის პირველად ანალიზს და შეფასებას (გაზომვას);

2.9. **რისკების მართვა** - ორგანიზაციის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

2.10. **რისკების მოპყრობა** - რისკის მართვის პროცესის ნაწილი, კერძოდ რისკის შეცვლის პროცესი, რომელიც შესაძლოა მოიცავდეს რისკის თავიდან აცილებას იმ აქტივობის დაწყებაზე ან გაგრძელებაზე უარის თქმით, რომელიც თავის მხრივ მოიცავს რისკის მიღებას ან გაზრდას შესაძლებლობების გამოყენების მიზნით, კერძოდ:

2.10.1. რისკის წყაროს მოცილებას;

2.10.2. ხდომილების შეცვლას;

2.10.3. შედეგების შეცვლას;

2.10.4. რისკის სხვა მხარესთან გაზიარებას;

2.10.5. რიკის გაცნობიერებულად შენარჩუნებას და რისკის თავიდან აცილებას;

2.11. **კონტროლის მექანიზმების გამოყენებადობის განაცხადი** - ორგანიზაციის იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

2.12. **პერსონალური მონაცემები** - ნებისმიერი ინფორმაცია, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (‘მონაცემთა სუბიექტს’); იდენტიფიცირებადი ფიზიკური პირი არის ის, ვისი პირდაპირ ან არაპირდაპირ იდენტიფიცირებაც შესაძლებელია ისეთი იდენტიფიკატორის გამოყენებით, როგორიცაა სახელი, პირადი ნომერი, ინფორმაცია ადგილმდებარეობის შესახებ, ონლაინ იდენტიფიკატორი ან ფიზიკური პირის იდენტობისათვის დამახასიათებელი ერთი ან მეტი ფიზიკური, ფსიქოლოგიური, გენეტიკური, გონებრივი, ეკონომიკური, კულტურული ან სოციალური ფაქტორით;

2.13. **მონაცემთა დამუშავება** - ნებისმიერი ქმედებაა ან ქმედებათა ერთობლიობა პერსონალურ მონაცემთან ან მონაცემთა ერთობლიობასთან მიმართებაში, ავტომატური თუ სხვა საშუალებებით, როგორიცაა მაგალითად შეგროვება, აღრიცხვა/ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, ამოღება, გაცნობა, გამოყენება, გამჟღავნება გადაცემის, გავრცელების ან ხელმისაწვდომობის სხვაგვარად უზრუნველყოფის გზით, დაჯგუფება ან კომბინირება, შეზღუდვა, წაშლა ან განადგურება;

2.14. **ინფორმაციული უსაფრთხოების ინციდენტი** - ინციდენტი, რომელიც არღვევს ან დაარღვევს ორგანიზაციის ინფორმაციული აქტივის (მათ შორის პერსონალური მონაცემების) კონფიდენციალურობას, მთლიანობას, ხელმისაწვდომობას - შესაბამისად მოითხოვს სპეციალური ღონისძიებების განხორციელებას;

3. მიზნები და ამოცანები

3.1. ინფორმაციული უსაფრთხოების პოლიტიკის მიზანია ორგანიზაციაში ინფორმაციული უსაფრთხოების და მონაცემთა დაცვის უზრუნველყოფისთვის საჭირო ძირითადი პრინციპებისა და მიდგომების განსაზღვრა;

3.2. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნებია:

3.2.1. კომპანია იუჯითის პროდუქტების ხარისხის განვითარების, ბიზნეს პროცესების უწყვეტობის, ბიზნეს რისკების შემცირების, ფინანსური რესურსების ეფექტურად მართვისა და საქმიანობის კანონშესაბამისობის უზრუნველყოფის ხელშეწყობა.

3.2.2. ინფორმაციული უსაფრთხოების პოლიტიკის და სხვა შიდა მარეგულირებელი წესების ეფექტიანი განხორციელება;

4. გავრცელების სფერო

ინფორმაციული უსაფრთხოების პოლიტიკა ვრცელდება:

4.1.1. კომპანია იუჯითი ჯგუფისა და კომპანია იუჯითის ყველა თანამშრომელზე;

4.1.2. კომპანია იუჯითი ჯგუფისა და კომპანია იუჯითის ყველა ბიზნეს პროცესზე.

4.1.3. იუჯითის თანამშრომლებსა/სტაჟიორებსა და მესამე პირებზე, რომელთაც წვდომა აქვთ ორგანიზაციის ინფორმაციულ აქტივებზე ან მონაწილეობენ მათ დამუშავებაში.

პასუხისმგებლობები

4.2. ორგანიზაციის თანამშრომლები, სტაჟიორები და მესამე მხარის წარმომადგენლები ვალდებულები არიან შეასრულონ ინფორმაციული უსაფრთხოების პოლიტიკიდან გამომდინარე მოთხოვნები და ინფორმაციული უსაფრთხოების შემჩნეული შეუსაბამობების შესახებ, დაუყოვნებლივ შეატყობინონ ინფორმაციული უსაფრთხოების მენეჯერს.

4.3. მოცემული პოლიტიკა განსაზღვრავს პირებს და ერთეულებს, რომლებიც განახორციელებენ ინფორმაციული უსაფრთხოების მართვას და მის კონტროლს.

4.4. მენეჯმენტის ვალდებულებები:

4.4.1. ორგანიზაციის მენეჯმენტი უზრუნველყოფს მართვის სისტემის და მისი გავრცელების სფეროში მოქცეული პროცესებისა და სტრუქტურული ერთეულების მხარდასაჭერად საჭირო ადამიანური, ფინანსური და ტექნიკური რესურსების ხელმისაწვდომობას.

4.4.2. ორგანიზაციის მენეჯმენტი უზრუნველყოფს, რომ განხორციელდება ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტირება, გავრცელების ფარგლების დადგენა, დაგეგმვა, იმპლემენტაცია, მონიტორინგი და მუდმივი გაუმჯობესება.

5. ინფორმაციული უსაფრთხოების საბჭო

5.1. ორგანიზაციის ხელმძღვანელობა აყალიბებს, ინფორმაციული უსაფრთხოების საბჭოს, რომელიც შედგება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისგან, რომლებიც უშუალოდ განახორციელებენ იუმს-ის მართვასა და მის მიმოხილვას.

5.2. ინფორმაციული უსაფრთხოების საბჭო განახორციელებს იუმს-ის მიმოხილვას დაგეგმილი პერიოდულობით (სულ მცირე წელიწადში ერთხელ):

5.2.1. რათა უზრუნველყოფილი იყოს ადეკვატური გავრცელების სფერო და იუმს-ს პროცესის გაუმჯობესებების აღმოჩენა;

5.2.2. რათა უზრუნველყოფილი იყოს მუდმივი შესაბამისობა, ადეკვატურობა და ეფექტიანობა;

5.3. მიმოხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვლილებების საჭიროებას, მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკას და მიზნებს.

5.4. მიმოხილვის შედეგები უნდა იყოს დოკუმენტირებული და ხდებოდეს ჩანაწერების წარმოება.

6. ინფორმაციული უსაფრთხოების მენეჯერი

6.1. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია ინფორმაციული უსაფრთხოების საბჭოს წინაშე.

6.2. ინფორმაციული უსაფრთხოების მენეჯერი ვალდებულია ყველა ინიციატივა, რომელიც შეეხება ინფორმაციული უსაფრთხოების მართვის სისტემას, შესაბამისი გადაწყვეტილების მისაღებად წარუდგინოს ინფორმაციული უსაფრთხოების სამუშაო ჯგუფს.

6.3. ინფორმაციული უსაფრთხოების მენეჯერის მოვალეობები განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით.

7. მესამე მხარე

7.1. ყველა მესამე მხარე (მათ შორის კონტრაქტორი, მომწოდებელი), რომელსაც აქვს ან ექნება ორგანიზაციის კუთვნილ ინფორმაციული აქტივებისადმი წვდომა ან/და მიიღებს მონაწილეობას მათ დამუშავება/შენახვაში, ვალდებულია გაეცნოს ინფორმაციული უსაფრთხოების პოლიტიკას და შეასრულოს პოლიტიკიდან გამომდინარე მოთხოვნები.

8. აქტივების მართვა

8.1. კომპანია ახორციელებს დადგენილ გავრცელების სფეროში გამოვლენილი აქტივების მართვას, რაც გულისხმობს აქტივების აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და უზრუნველყოფას.

8.2. ყოველ აქტივს გააჩნია მასზე პასუხისმგებელი პირი ან სტრუქტურული ერთეული - აქტივის მფლობელი.

8.3. ინფორმაციული აქტივების მართვის წესები განისაზღვრება გენერალური დირექტორის ბრძანებით.

9. რისკების მართვა

9.1. კომპანიის ინფორმაციული უსაფრთხოების მართვის სისტემა დაფუძნებულია რისკების იდენტიფიცირების და მართვის პროცესებზე:

9.1.1. კომპანია განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების შეფასების მიდგომას;

9.1.2. კომპანია გამოავლენს ინფორმაციული უსაფრთხოების რისკებს და გაანალიზებს მათი გავლენას კომპანიის საქმიანობაზე;

9.1.3. კომპანია ჩაატარებს გამოვლენილი რისკების ანალიზს და შეფასებას;

9.1.4. კომპანია რისკების მოპყრობის მიზნით შეარჩევს კონტროლის მიზნებს და კონტროლის მექანიზმებს;

9.1.5. კომპანია განსაზღვრავს მისაღები რისკის დონეს;

9.2. რისკების მოპყრობის გეგმა განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო ქმედებებს საბჭოს მხრიდან, რესურსებს, პასუხისმგებლობებს და პრიორიტეტებს.

10. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

10.1. კომპანია მოამზადებს კონტროლის მექანიზმების გამოყენებადობის განაცხადს, რომელიც შეიცავს:

10.1.1. ინფორმაციული უსაფრთხოების მოთხოვნებისთვის შერჩეული კონტროლის მიზნებს და კონტროლის მექანიზმებს, ასევე მათი შერჩევის დასაბუთებას;

10.1.2. კომპანიაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

10.1.3. უარყოფილი (კონტროლის მექანიზმები რომლის გამოყენებაც არ მოხდა) კონტროლების მიზნის და კონტროლის მექანიზმების ჩამონათვალს და გამორიცხვის დასაბუთებას.

10.2. კომპანია უზრუნველყოფს კონტროლის მექანიზმების მიზნების მიღწევას, და შესაბამისი პასუხისმგებლობების და როლების განსაზღვრას.

10.3. იუმს-ის მიზნების მისაღწევად ორგანიზაცია:

10.3.1. დანერგავს შერჩეულ კონტროლის მექანიზმებს;

10.3.2. განახორციელებს ISO/IEC 27017:2015-ის მიხედვით ღრუბლოვანი სერვისების ფარგლებში მომხმარებლების უსაფრთხოებისთვის შესაბამისი გარემოს იზოლირების, ვირტუალიზაციის უსაფრთხოების და ანგარიშების სასიცოცხლო ციკლის მართვისათვის შესაბამისი კონტროლის მექანიზმების დანერგვას.

10.3.3. განახორციელებს ISO/IEC 27018:2019-ის მიხედვით პერსონალური იდენტიფიცირებადი ინფორმაციის (PII) დაცვის ღონისძიებებს ISO/IEC 29100-ის კონფიდენციალურობის პრინციპების შესაბამისად საჯარო ღრუბლოვანი გამოთვლითი გარემოსთვის.

10.3.4. კონტროლის მექანიზმების დანერგვისთანავე აწარმოებს მათზე დაკვირვებას;

10.3.5. გაანალიზებს დაკვირვების შედეგებს და საჭიროების შემთხვევაში, დააღგენს სამოქმედო გეგმას.

11. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა

11.1. კომპანია უზრუნველყოფს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის უახლესი ვერსიის ხელმისაწვდომობას ყველა უფლებამოსილი პირისთვის, ასევე იუმს-ის დოკუმენტაციის სათანადოდ დაცვასა და კონტროლს.

11.2. კომპანია აწარმოებს იუმს-ის ფარგლებში ჩანაწერებს და უზრუნველყოფს მათ მხარდაჭერას იუმს-ის მოთხოვნებთან შესაბამისობისა და ეფექტიანი ფუნქციონირების მიზნით. ჩანაწერები უნდა იყოს სათანადოდ დაცული და უნდა ხორციელდებოდეს მისი შესაბამისი კონტროლი.

12. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

12.1. კომპანია შეიმუშავებს და განახორციელებს ინფორმაციული უსაფრთხოების სატრენინგო და ცნობიერების ამაღლების პროგრამებს.

12.2. კომპანია უზრუნველყოფს პერსონალის კვალიფიციურობას იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

12.2.1. განსაზღვრავს იუმს-ში ჩართული პერსონალისთვის აუცილებელ ცოდნის დონეს;

12.2.2. ჩაატარებს ტრენინგებს და სხვა ღონისძიებებს (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

12.2.3. აწარმოებს ჩანაწერებს სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ.

12.3. კომპანია უზრუნველყოფს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ წვლილს.

13. ინფორმაციული უსაფრთოხების ინციდენტების მართვა

13.1. ბიზნეს პროცესების უწყვეტობის, საოპერაციო ხარჯების ეფექტურად გამოყენების, ასევე კომპანიის პროდუქტების და მომსახურების ხარისხის გაუმჯობესების ხელშეწყობის მიზნით, კომპანია ახორციელებს ინფორმაციული უსაფრთხოების ინციდენტების მართვას.

13.2. ინციდენტების მართვა მოიცავს ინციდენტების იდენტიფიცირების, ანგარიშგების, აგრეთვე რეაგირების პროცედურებსა და საშუალებებს.

13.3.კომპანია უზრუნველყოფს ინციდენტების შესახებ დაინტერესებულ მხარეებთან კომუნიკაციას „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით დადგენილი წესების შესაბამისად.

14. ბიზნეს უწყვეტობის მართვა

14.1. კომპანია ახორციელებს ინფორმაციული უსაფრთხოების ასპექტებზე ბიზნეს პროცესების გავლენის ანალიზს, რის შესაბამისად ადგენს ინფორმაციული უსაფრთხოების მოთხოვნების მიხედვით უწყვეტობის გეგმებს, რომელიც საშუალებას აძლევს ორგანიზაციას კრიზისული სიტუაციების და კატასტროფის დროს აღადგინოს ყველა საჭირო სერვისი დროის მოკლე მონაკვეთში.

14.2. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნებისთვის, ორგანიზაცია განსაზღვრავს ინფორმაციული უსაფრთხოებისა უწყვეტობის კრიტერიუმებს, როლებს და პასუხისმგებლობებს, პროცედურებს მსხვილი ინციდენტის დადგომისას და სერვისის ხელმისაწვდომობის სამიზნე მაჩვენებლებს.

15. კომუნიკაცია

15.1. ინფორმაციული უსაფრთხოების პოლიტიკის ხელმისაწვდომობა უზრუნველყოფილია ყველა დაინტერესებული მხარისათვის შესაბამისი ფორმით;

15.2. ინფორმაციული უსაფრთხოების პოლიტიკაში ცვლილებების შესახებ ინფორმაცია ეცნობება დაინტერესებულ მხარეებს, შესაბამისი ფორმით.

15.3. პოლიტიკის ცვლილებების ან უსაფრთხოების სხვა საკითხებთან დაკავშირებით დაინტერესებული მხარეების შეტყობინებაზე პასუხისმგებელია ინფორმაციული უსაფრთხოების მენეჯერი.

16. იუმს-ის აუდიტი და უსაფრთხოების დონის შეფასება

16.1. კომპანია ატარებს იუმს-ის აუდიტს დაგეგმილი პერიოდულობით და ადგენს:

16.1.1. შეესაბამება თუ არა სტანდარტსა და საკანონმდებლო მოთხოვნებს;

16.1.2. შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

16.2. შესაბამის პირებს, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და მათი გამომწვევი მიზეზების აღმოფხვრა.

16.3.ორგანიზაცია დადგენილი პერიოდულობით ატარებს ინფორმაციული სისტემების შეღწევადობის ტესტირებას და სისუსტეების სკანირებას, რომელიც მიზნად ისახავს სისტემებში არსებული არასწორი კონფიგურაციის/სისუსტეების გამოვლენას;

16.4.ტესტირების შედეგად გამოვლენილი სისუსტეების აღმოსაფხვრელად ორგანიზაცია ამზადებს სამოქმედო გეგმას და უზრუნველყოფს აღმოფხვრის პროცესის ეფექტიან განხორციელებას.

17. ინფორმაციული უსაფრთხოების გაზომვადი ამოცანები

17.1.ინფორმაციული უსაფრთხოების მართვის სისტემის მაღალი დონის მიზნების და ამოცანების მისაღწევად კომპანიას დადგენილი აქვს ინფორმაციული უსაფრთხოების მართვის სისტემის გაზომვადი საოპერაციო ამოცანები;

17.2.გაზომვადი ამოცანები წელიწადში ერთხელ ინიცირდება ინფორმაციული უსაფრთხოების მენეჯერის მიერ.

17.3.გაზომვადი ამოცანების შესრულების კონტროლზე პასუხისმგებელია ინფორმაციული უსაფრთოხების საბჭო და შესრულება განიხილება საბჭოს სხდომაზე;

18. მუდმივი გაუმჯობესება

18.1. კომპანია პერიოდულად განიხილავს იუმს-ის ეფექტიანობას (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვას). პერიოდული მიმოხილვის დროს ორგანიზაცია გაითვალისწინებს ინფორმაციული უსაფრთხოების აუდიტის შედეგებს, ინციდენტებს, ეფექტიანობის გაზომვის შედეგებს და დაინტერესებული მხარეებისგან მიღებულ შემოთავაზებებსა და უკუკავშირს.

18.2. ინფორმაციული უსაფრთხოების მენეჯერი, ინფორმაციული უსაფრთოხების საბჭო და ინფორმაციული უსაფრთოხების უზრუნველყოფაში ჩართული ყველა რგოლი მუდმივად მუშაობს მართვის სისტემისა და უსაფრთოხების გაუმჯობესებაზე შემდეგი ძირითადი მეთოდების საშუალებით:

18.2.1. საკვანძო პარამეტრების დადგენა, მისი მონიტორინგი და შესრულების კონტროლი;

18.2.2. პროცესების პერიოდული (დაგეგმილი) აუდიტი ISO/IEC 27001 სტანდარტის შესაბამისად;

18.2.3. დადგენილი პერიოდულობით რისკების შეფასების ჩატარება და შედეგების შესაბამისი სამშოების გატარება;

19. პოლიტიკის გადახედვა

მოცემული პოლიტიკა ექვემდებარება გადახედვას მინიმუმ წელიწადში ერთხელ ან კომპანიაში მნიშვნელოვანი ცვლილებებისამებრ და საჭიროების შემთხვევაში განხორციელდება ცვლილებების ან/და დამატებების შეტანა.