ინფორმაციული უსაფრთხოების პოლიტიკა

საქართველო, თბილისი
2021 წელი

ინფორმაცია დოკუმენტზე

ვერსია:	V3.0
ცვლილების თარიღი:	25.10.2021
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

სარჩევი

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 ISO27001:2013;

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

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

2.3. **ავტორიზებული ერთეული** - ინდივიდი, სუბიექტი ან პროცესი, რომელსაც გააჩნია აქტივზე წვდომის უფლება;

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

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

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

2.7. **ინფორმაციული უსაფრთხოება** - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, აუთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

2.8. **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;

2.9. რეაგირების გარეშე **ნარჩენი რისკი** - რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

2.10. **რისკის მიღება** - გადაწყვეტილება რისკის მიღების თაობაზე;

2.11. **რისკის ანალიზი** - ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მისი შეფასების დასადგენად;

2.12. **რისკის დონის დადგენა** - რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

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

2.14. **რისკების მოპყრობა** - რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

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

3. მიზნები და ამოცანები

3.1. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნებია:

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

3.1.2. ISO/IEC 27001:2013 ინფორმაციული უსაფრთხოების სტანდარტთან თავსებადი ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვა.

3.1.3. ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და პოლიტიკის ეფექტიანი განხორციელება;

4. გავრცელების სფერო

ინფორმაციული უსაფრთხოების პოლიტიკა ვრცელდება:

4.1. კომპანია იუჯითი ჯგუფისა და კომპანია იუჯითის ყველა თანამშრომელზე;
4.2. კომპანია იუჯითი ჯგუფისა და კომპანია იუჯითის ყველა ბიზნეს პროცესზე.

5. პასუხისმგებლობები

5.1. ორგანიზაციის თანამშრომლები, სტაჟიორები და მესამე მხარის წარმომადგენლები ვალდებულები არიან შეასრულოს ინფორმაციული უსაფრთხოების პოლიტიკიდან გამომდინარე მოთხოვნები და ინფორმაციული უსაფრთხოების შემჩნეული შეუსაბამობების შესახებ, დაუყოვნებლივ შეატყობინოს ინფორმაციული უსაფრთხოების სამუშაო ჯგუფს.
5.2. მოცემული პოლიტიკა განსაზღვრავს პირებს და ერთეულებს, რომლებიც განახორციელებენ ინფორმაციული უსაფრთხოების მართვას და მის კონტროლს.
5.3. მენეჯმენტის ვალდებულებები:
5.3.1. ორგანიზაციის მენეჯმენტი უზრუნველყოფს მართვის სისტემის და მისი გავრცელების სფეროში მოქცეული პროცესებისა და სტრუქტურული ერთეულების მხარდასაჭერად საჭირო ადამიანური, ფინანსური და ტექნიკური რესურსების ხელმისაწვდომობას.
5.3.2. ორგანიზაციის მენეჯმენტი უზრუნველყოფს, რომ განხორციელდება ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტირება, გავრცელების ფარგლების დადგენა, დაგეგმვა, იმპლემენტაცია, მონიტორინგი და მუდმივი გაუმჯობესება.

6. ინფორმაციული უსაფრთხოების საბჭო

6.1. ორგანიზაციის ხელმძღვანელობა აყალიბებს, ინფორმაციული უსაფრთხოების საბჭოს, რომელიც შედგება ინფორმაციული უსაფრთხოების ოფიცრის და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისგან, რომლებიც უშუალოდ განახორციელებენ იუმს-ის მართვასა და მის მიმოხილვას.
6.2. ინფორმაციული უსაფრთხოების საბჭო განახორციელებს იუმს-ის მიმოხილვას დაგეგმილი პერიოდულობით (სულ მცირე წელიწადში ერთხელ):
6.2.1. რათა უზრუნველყოფილი იყოს ადეკვატური გავრცელების სფერო და იუმს-ს პროცესის გაუმჯობესებების აღმოჩენა;
6.2.2. რათა უზრუნველყოფილი იყოს მუდმივი შესაბამისობა, ადეკვატურობა და ეფექტიანობა;
6.3. მიმოხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვლილებების საჭიროებას, მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკას და მიზნებს.
6.4. მიმოხილვის შედეგები უნდა იყოს დოკუმენტირებული და ხდებოდეს ჩანაწერების წარმოება.

7. ინფორმაციული უსაფრთხოების სამუშაო ჯგუფი

7.1. ინფორმაციული უსაფრთხოების სამუშაო ჯგუფს ხელმძღვანელობს ინფორმაციული უსაფრთხოების ოფიცერი;

7.2. ჯგუფის მოვალეობა არის ინფორმაციულ უსაფრთხოებასთან დაკავშირებული საკითხების განხილვა, შეთანხმება და საბჭოსთვის წარდგენა დასამტკიცებლად.

7.3. ინფორმაციული უსაფრთხოების საბჭო წარადგენს, ინფორმაციული უსაფრთხოების სამუშაო ჯგუფის წევრებს და გენერალური დირექტორი ამტკიცებს შემადგენლობას.

8. ინფორმაციული უსაფრთხოების ოფიცერი

8.1. ინფორმაციული უსაფრთხოების ოფიცერი ანგარიშვალდებულია ინფორმაციული უსაფრთხოების საბჭოს წინაშე.

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

8.3. ინფორმაციული უსაფრთხოების ოფიცრის მოვალეობები განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით.

9. მესამე მხარე

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

10. აქტივების მართვა

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

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

10.3. ინფორმაციული აქტივების მართვის წესები განისაზღვრება გენერალური დირექტორის ბრძანებით.

11. რისკების მართვა

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

11.1.1. კომპანია განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების შეფასების მიდგომას;

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

11.1.3. კომპანია ჩაატარებს გამოვლენილი რისკების ანალიზს და შეფასებას;

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

11.1.5. კომპანია განსაზღვრავს მისაღები რისკის დონეს;

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

12. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

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

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

12.1.2. კომპანიაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

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

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

12.3. იუმს-ის მიზნების მისაღწევად ორგანიზაცია:

12.3.1. დანერგავს შერჩეულ კონტროლის მექანიზმებს;

12.3.2. კონტროლის მექანიზმების დანერგვისთანავე აწარმოებს მათზე დაკვირვებას;

12.3.3. გაანალიზებს დაკვირვების შედეგებს და საჭიროების შემთხვევაში, დაადგენს სამოქმედო გეგმას.

13. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა

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

13.2. 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.

14. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

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

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

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

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

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

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

15. ინფორმაციული უსაფრთოხების ინციდენტების მართვა

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

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

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

16. კომუნიკაცია

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

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

16.3. პოლიტიკის ცვლილებების ან უსაფრთხოების სხვა საკითხებთან დაკავშირებით დაინტერესებული მხარეების შეტყობინებაზე პასუხისმგებელი პირები მოცემულია კომუნიკაციის გეგმაში;

17. იუმს-ის აუდიტი

17.1. კომპანია ჩაატარებს იუმს-ის აუდიტს დაგეგმილი პერიოდულობით და დაადგენს:

17.1.1. შეესაბამება თუ არა სტანდარტსა და საკანონმდებლო მოთხოვნებს;

17.1.2. შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

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

18. მუდმივი გაუმჯობესება

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

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

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

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

19. პოლიტიკის გადახედვა

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