მაგთიკომის

ინფორმაციული უსაფრთხოების პოლიტიკა

2022 წელი

ინფორმაციული უსაფრთხოების პოლიტიკა

1. შინაარსი

1.1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის თანახმად დადგენილია კრიტიკული ინფორმაციის სისტემის სუბიექტების სამი კატეგორია. კანონის მიხედვით მეორე კატეგორიის კრიტიკული ინფორმაციის სისტემის სუბიექტს წარმოადგენს სატელეკომუნიკაციო სექტორის ორგანიზაციები. საქართველოს მთავრობის 2021 წლის 31 დეკემბრის N646 დადგენილებით შპს “მაგთიკომი“ (საიდ. ნომერი: 204876606, მის: პოლიტკოვსკაიას ქ. N7, 0186 თბილისი, საქართველო) წარმოადგენს მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს.

1.2. მაგთიკომის მიზნების ეფექტიანად განხორციელებისთვის მნიშვნელოვანია ორგანიზაციის ინფორმაციული აქტივების უსაფრთხოების უზრუნველყოფა და სათანადო დონეზე დაცვა (კონფიდენციალობა, ხელმისაწვდომობა და მთლიანობა), რასაც სხვა საშუალებებთან ერთად აღწევს ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვით.

1.3. მაგთიკომის ინფორმაციული უსაფრთხოების მართვის სისტემა შედგება: პოლიტიკებისგან, პროცედურებისგან, სახელმძღვანელო მითითებებისგან, დაკავშირებული რესურსებისა და აქტივობებისაგან, რომელთაც ორგანიზაცია მართავს კოლექტიურად მისი ინფორმაციული აქტივების დასაცავად.

1.4. მაგთიკომის ინფორმაციული უსაფრთხოების პოლიტიკა აღწერს ინფორმაციული უსაფრთხოების მართვის სისტემის ფუნქციონირების ძირითად პრინციპებს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის და ISO/IEC 27001 სტანდარტის შესაბამისად.

2. ტერმინთა განმარტება

ამ პოლიტიკის მიზნებისთვის მასში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

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

2.2. **ინფორმაციული 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;

2.3. **ინფორმაციული უსაფრთხოების მართვის სისტემა** - მართვის სისტემის ნაწილი, რომელიც წარმოადგენს ორგანიზაციის ინფორმაციული უსაფრთხოების დაფუძნების, აღსრულების, მართვის, მონიტორინგის, გადახედვის, შენარჩუნების და გაუმჯობესების სისტემური მიდგომას. ინფორმაციული უსაფრთხოების მართვის სისტემა ეფუძნება ორგანიზაციის მიერ რისკის შეფასების და რისკის მიღების კრიტერიუმებს, რომლებიც შემუშავებულია რისკების ეფექტიანი მოპყრობისა და მართვისთვის.

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. **ორგანიზაცია** - შპს მაგთიკომი;

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 შეცვლის პროცესი, რომელიც შესაძლოა მოიცავდეს რისკის თავიდან აცილებას იმ აქტივობის დაწყებაზე ან გაგრძელებაზე უარის თქმით, რომელიც თავის მხრივ მოიცავს:

- შესაძლოა მოიცავდეს რისკის მიღებას ან გაზრდას შესაძლებლობების გამოყენების მიზნით, კერძოდ:
- რისკის წყაროს მოცილებას;
- ხდომილების შეცვლას;
- შედეგების შეცვლას;
- რისკის სხვა მხარესთან გაზიარებას;
- რიკის გაცნობიერებულად შენარჩუნებას და რისკის თავიდან აცილებას;

2.11. **პასუხისმგებელი პირი** - აქტივთან, რისკთან ან სხვა მიმართებაში პასუხისმგებელ პირად შეიძლება განისაზღვროს როგორც კონკრეტული როლი და პირი, ასევე სტრუქტურული ერთეული.

3. ინფორმაციული უსაფრთხოების პოლიტიკის მიზანი

ინფორმაციული უსაფრთხოების პოლიტიკის მიზანია ორგანიზაციაში ინფორმაციული უსაფრთხოების უზრუნველყოფისთვის საჭირო ძირითადი პრინციპებისა და მიდგომების განსაზღვრა;

4. პოლიტიკის მოქმედების სფერო

4.1. ინფორმაციული უსაფრთხოების პოლიტიკა ვრცელდება ორგანიზაციის:

4.1.1. ყველა თანამშრომელზე (მათ შორის სტაჟიორებზე);

4.1.2. ყველა ბიზნეს პროცესზე (ძირითად და მხარდამჭერ პროცესებზე);

4.1.3. ყველა ტიპის ინფორმაციულ აქტივზე;

4.1.4. მესამე პირებზე, რომელთაც წვდომა აქვთ ორგანიზაციის ინფორმაციულ აქტივებზე ან მონაწილეობენ მათ დამუშავებაში.

4.2. მოქმედების სფეროს დაზუსტებულია ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტში.

5. ინფორმაციული უსაფრთხოების საბჭო

5.1. ორგანიზაცია ქმნის ინფორმაციული უსაფრთხოების საბჭოს, რომლის მიზანია ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანი ფუნქციონირება, შესაბამისობა და ადეკვატურობა.

5.2. ინფორმაციული უსაფრთხოების საბჭოს მიზანი, ამოცანები ფუნქციები, საბჭოს შემადგენლობა, საბჭოს რეგლამენტი და ორგანიზაციულ-ტექნიკური მხარდაჭერის დეტალები ასახულია საბჭოს დებულებაში (ინფორმაციული უსაფრთხოების საბჭოს დებულება).

6. ინფორმაციული უსაფრთხოების მენეჯერი

6.1. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია ინფორმაციული უსაფრთხოების საბჭოსთან;

6.2. ინფორმაციული უსაფრთხოების მენეჯერის ვალდებულებები და ფუნქციები განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით, „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერებისთვის მინიმალური სტანდარტების დადგენის შესახებ“ სსიპ საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2022 წლის 03 მაისის N 12 ბრძანებით და სამუშაო აღწერილობით, რომელიც მოიცავს:

6.2.1. ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;

6.2.2. ინფორმაციული აქტივებისა და მათი წვდომის აღწერა;

6.2.3. ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის (პოლიტიკები, ინსტრუქციები, სახელმძღვანელოები და ა.შ.) პროექტების მომზადების, დამტკიცების და გადახედვის პროცესების კოორდინაცია;

6.2.4. ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვება და მათზე რეაგირების მონიტორინგი;

6.2.5. ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობა;

6.2.6. ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება;

6.2.7. სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი;

6.2.8. სამოქმედო გეგმის შედგენა და ამ გეგმის შესრულების ყოველწლიური ანგარიშის ზემოთ ნახესენები სტანდარტების მე-2 მუხლის მე-2 პუნქტით განსაზღვრული პირებისთვის და სააგენტოსთვის წარდგენა;

6.2.9. ინფორმაციული უსაფრთხოების საბჭოსთან შეთანხმებით ორგანიზაციის ქსელურ სენსორზე ან/და ორგანიზაციის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის დაშვება და აღნიშნული გადაწყვეტილების თაობაზე შეტყობინება.

7. მესამე მხარეები

7.1. მესამე მხარე (მათ შორის კონტრაქტორი ორგანიზაციის წარმომადგენელი, მომწოდებელი ორგანიზაციის უფლებამოსილი პირი), რომელსაც ექნება წვდომა ორგანიზაციის კუთვნილ ინფორმაციულ აქტივზე ან/და მიიღებს მონაწილეობას მათ დამუშავებაში, ვალდებულია გაეცნოს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას და შეასრულოს პოლიტიკის რეგულაციები.

8. აქტივების მართვა

8.1. ორგანიზაცია უზრუნველყოფს ინფორმაციული აქტივების იდენტიფიკაციას და კლასიფიკაციას, ასევე მათი შეცვლისა და განადგურების წესების დადგენას.

8.2. იდენტიფიცირებულ ყოველ აქტივის მიმართ განსაზღვრულია პასუხისმგებელი პირი.

8.3. ინფორმაციული აქტივების იდენტიფიცირებისა და კლასიფიკაციის წესები განსაზღვრულია ინფორმაციული აქტივების იდენტიფიცირებისა და კლასიფიკაციის მეთოდოლოგიაში;

9. რისკების მართვა

9.1. ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემა დაფუძნებულია ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში, პროცესის ფარგლებში ორგანიზაცია:

9.1.1. განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირებისა და შეფასების მიდგომებს;

9.1.2. გამოავლენს ინფორმაციული უსაფრთხოების რისკებს და გაანალიზებს მათ გავლენას და ჩაატარებს რისკების ანალიზს;

9.1.3. რისკების მოპყრობის მიზნით შეარჩევს საჭირო კონტროლის მექანიზმებს და განსაზღვრავს მისაღები რისკის დონეს;

9.1.4. მოამზადებს რისკების მოპყრობის გეგმას.

9.2. რისკების მართვის პროცესის დეტალები მოცემულია რისკების იდენტიფიცირებისა და შეფასების მეთოდოლოგიაში.

10. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

10.1. ინფორმაციის უსაფრთხოების მენეჯერი 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. ორგანიზაციაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

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

10.1.4. ორგანიზაცია უზრუნველყოფს კონტროლის მექანიზმების მიზნების მიღწევას, რაც გულისხმობს ეფექტურობისა და რესურსების განაწილებას, ასევე საჭირო როლებისა და პასუხისმგებლობების განსაზღვრას.

10.2. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნების მისაღწევად ორგანიზაცია:

10.2.1. დანერგავს შერჩეულ კონტროლის მექანიზმებს;

10.2.2. კონტროლის მექანიზმების დანერგვის შემდგომ აწარმოებს მათზე დაკვირვებას;

10.2.3. გაანალიზებს დაკვირვების შედეგებს და საჭიროების შემთხვევაში განსაზღვრავს სამოქმედო გეგმას.

11. ცნობიერების ამაღლება და კომპეტენციების განვითარება

11.1. ორგანიზაცია შეიმუშავებს და განახორციელებს ინფორმაციული უსაფრთხოების ცნობიერების ამაღლების პროგრამებს, ასევე მუდმივად იზრუნებს თანამშრომელთა კომპეტენციების განვითარებაზე.

11.2. ორგანიზაციის მიდგომები ცნობიერების ამაღლებაზე და კომპეტენციების განვითარების მიმართულებით ორგანიზაცია:

11.2.1. განსაზღვრავს ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების ფარგლებში მოქცეული თანამშრომლების ცოდნის დონეს;

11.2.2. ჩაატარებს ტრენინგებს და სხვადასხვა აქტივობებს ინფორმაციული უსაფრთხოების მოთხოვნების დასაკმაყოფილებლად;

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

11.2.4. შეაფასებს პერსონალის ცოდნის და ცნობიერების დონეს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელობაზე.

11.2.5. წარმოაჩანს თანამშრომელთა პირად პირადი პასუხისმგებლობას საკუთარ მოქმედებაზე ან უმოქმედობაზე და ზოგადი ვალდებულებები ორგანიზაციის კუთვნილი ინფორმაციის დაცვაზე;

11.2.6. თანამშრომელთათვის ხელმისაწვდომს გახდის და მიუთითებს ინფორმაციის დამატებითი წყაროებზე და ასევე საკონტაქტო ინფორმაციის ყველა საჭირო მიმართულებით.

11.3. ცნობიერების ამაღლების პროგრამების დაგეგმვა ხდება ორგანიზაციაში დასაქმებულის როლისა და ვალდებულებების გათვალისწინებით, რათა უზრუნველყოფილი იყოს პოლიტიკებით, სტანდარტებით, საკანონმდებლო აქტებით და ხელშეკრულებებით განსაზღვრული ინფორმაციული უსაფრთხოების წესების და ვალდებულებების ცოდნა და დაცვა.

11.4. ცნობიერების ამაღლების პროგრამების განახლება უნდა განხორციელდეს პერიოდულად, ორგანიზაციის პოლიტიკებისა და პროცედურების შესაბამისად, წელიწადში არანაკლებ ერთხელ.

12. ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტების მართვა

12.1. ორგანიზაცია იზრუნებს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის (ელექტრონული ფორმით) უახლესი ვერსიის ხელმისაწვდომობას ყველა დაინტერესებული პირისთვის, ასევე უზრუნველყოფს მართვის სისტემის დოკუმენტაციის სათანადოდ დაცვასა და კონტროლს.

12.2. ორგანიზაცია ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლებში აწარმოებს სათანადო ჩანაწერებს, უზრუნველყოფს მათ მხარდაჭერას, დაცვას და კონტროლს მართვის სისტემის მოთხოვნების შესაბამისად, დეტალური ინფორმაცია მოცემულია დოკუმენტების კონტროლის პროცედურაში.

13. ინფორმაციული უსაფრთხოების ინციდენტების მართვა

13.1. ორგანიზაცია უზრუნველყოფს ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცესის ეფექტიან განხორციელებას, რომელსაც წარმართავს კომპიუტერული უსაფრთხოების სპეციალისტი;

13.2. ინფორმაციული უსაფრთხოების ყველა ინციდენტი აღირიცხება და მუშავდება დადგენილი წესის შესაბამისად.

13.3. ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცესი მოიცავს ინციდენტის იდენტიფიცირების, რეაგირების, ჩანაწერების შეგროვების, აღმოფხვრის, განხილვის და ცოდნის გაზიარების ეტაპებს.

13.4. ორგანიზაცია უზრუნველყოფს ინციდენტების შესახებ დაინტერესებულ მხარეებთან კომუნიკაციას კანონით დადგენილი წესების შესბამისად.

14. ბიზნეს უწყვეტობის მართვა

14.1. ორგანიზაცია განახორციელებს ინფორმაციული უსაფრთხოების ასპექტებზე ბიზნეს პროცესების გავლენის ანალიზს და რის შესაბამისადაც დაადგენს ინფორმაციული უსაფრთხოების მოთხოვნების მიხედვით უწყვეტობის გეგმებს, რომელიც საშუალებას მისცემს 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. ინფორმაციული უსაფრთხოების მართვის სისტემის შიდა აუდიტი

15.1. ორგანიზაცია დადგენილი პერიოდულობით ჩაატარებს ინფორმაციული უსაფრთხოების მართვის სისტემის აუდიტს და დაადგენს სისტემის შესაბამისობას:

15.1.1. საკანონმდებლო და სტანდარტის მოთხოვნებთან;

15.1.2. ინფორმაციული უსაფრთხოების მოთხოვნებთან.

15.2. აუდიტის ეფექტურად განხორციელებისათვის, ორგანიზაცია შეიმუშავებს აუდიტის პროგრამებს, კრიტერიუმებსა და თითოეული აუდიტის ფარგლებს.

აუდიტის პროგრამები მხედველობაში უნდა იღებდეს შესაბამისი პროცესების მნიშვნელობას და წინა აუდიტების შედეგებს.

15.3. აუდიტის განსახორციელებლად ორგანიზაცია შეარჩევს ისეთ აუდიტორებს და ხელს შეუწყობს აუდიტის იმგვარ პროცესს, რომელიც დააკმაყოფილებს აუდიტის პროცესის დამოუკიდებლობისა და მიუკერძოებლობის მოთხოვნებს.

15.4. აუდიტის შედეგი განსახილველად წარედგინება ინფორმაციული უსაფრთხოების საბჭოს.

15.5. გამოვლენილი შეუსაბამობების აღმოსაფხვრელად, ორგანიზაცია მოამზადებს გეგმას და უზრუნველყოფს აღმოფხვრის პროცესის ეფექტიან განხორციელებას.

15.6. აუდიტის პროგრამებისა და აუდიტის შედეგების შესახებ დოკუმენტირებული ინფორმაცია შეინახება ინფორმაციული უსაფრთხიების საბჭოსთან შეთანხმებული ვადით.

16. ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

16.1. ორგანიზაცია დადგენილი პერიოდულობით ჩაატარებს ინფორმაციული სისტემების შეღწევადობის ტესტირებას, რომელიც მიზნად ისახავს სისტემებში არსებული არასწორი კონფიგურაციის/სისუსტეების გამოვლენას;

16.2. ტესტირების შედეგად გამოვლენილი სისუსტეების აღმოსაფხვრელად ორგანიზაცია მოამზადებს სამოქმედო გეგმას და უზრუნველყოფს აღმოფხვრის პროცესის ეფექტიან განხორციელებას.

16.3. პენეტრაციის ტესტი ან სისუსტეების შეფასება განხორციელდება მაქსიმალურად ფრთხილად და ექნება დაგეგმილი, დოკუმენტირებული და განმეორებადი ხასიათი.

16.4. პენეტრაციის ტესტი ან სისუსტეების შეფასება უნდა განხორციელდება მხოლოდ კომპეტენტური უფლებამოსილი პირის მიერ ან ამგვარი პირის ზედამხედველობით.

17. პოლიტიკის გადახედვის გეგმა

17.1. პოლიტიკის განახლებას, მუდმივ სრულყოფას და მის შესაბამისობას ორგანიზაციის მიზნებსა და ამოცანებთან უზრუნველყოფს ინფორმაციული უსაფრთხოების მენეჯერი;

17.2. პოლიტიკა უნდა გადაიხედოს არანაკლებ წელიწადში ერთხელ, ასევე ორგანიზაციაში განხორციელებული მნიშვნელოვანი ცვლილებების შემდგომ.

17.3. პოლიტიკის გადახედვა შესაძლებელია ასევე განხორციელდეს ბიზნეს გარემოს, სამართლებრივი ან/და ტექნიკური მოთხოვნების ცვლილების შესაბამისად.

18. დაკავშირებული დოკუმენტები

ინფორმაციული უსაფრთხოების პოლიტიკა დაკავშირებულია შემდეგ დოკუმენტებთან:

18.1. ინფორმაციული უსაფრთხოების გავრცელების სფეროს დოკუმენტი;

18.2. ინფორმაციული უსაფრთხოების საბჭოს დებულება;

18.3. ორგანიზაციული კონტექსტის დოკუმენტი.