Batumi International Container Terminal LLC
An ICTSI Group Company

ბათუმის საერთაშორისო საკონტეინერო ტერმინალის

ინფორმაციული უსაფრთხოების პოლიტიკა

ბაქოს ქ. 11, ბათუმი 6010
2022 წელი

ინფორმაცია დოკუმენტზე

დოკუმენტის დასახელება:	ინფორმაციული უსაფრთხოების პოლიტიკა		
ავტორი:	ნუკრი კაკაბაძე	**დოკუმენტის ვერსია:**	v1.0
თანამდებობა:	ინფორმაციული ტექნოლოგიების ოფიცერი	**ვერსიის თარიღი:**	27.12.2022
		გადახედვის თარიღი	
დამტკიცება:	ინფორმაციული უსაფრთხოების და ბიზნეს უწყვეტობის მმართველი კომიტეტი		

დოკუმენტის ისტორია

ვერსიის ნომერი	ვერსიის თარიღი	განმარტება
v1.0	27.12.2022	დოკუმენტის დამტკიცება

სარჩევი

ინფორმაციული უსაფრთხოების პოლიტიკა

1. შინაარსი

1.1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის თანახმად დადგენილია კრიტიკული ინფორმაციის სისტემის სუბიექტების სამი კატეგორია. საქართველოს მთავრობის 2021 წლის 31 დეკემბრის N646 დადგენილებით შპს “ბათუმის საერთაშორისო საკონტეინერო ტერმინალი“ წარმოადგენს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს.

1.2. ბათუმის საერთაშორისო საკონტეინერო ტერმინალის მიზნების ეფექტიანად განხორციელებისთვის მნიშვნელოვანია ორგანიზაციის ინფორმაციული აქტივების უსაფრთხოების უზრუნველყოფა და სათანადო დონეზე დაცვა (კონფიდენციალობა, ხელმისაწვდომობა და მთლიანობა).

1.3. ბათუმის საერთაშორისო საკონტეინერო ტერმინალის 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 დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

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 ბათუმის საერთაშორისო საკონტეინერო ტერმინალი;

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

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

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

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 პრინციპებისადა 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. გავრცელების სფერო დაზუსტებულია ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტში.

5. ინფორმაციული უსაფრთხოების საბჭო

5.1. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი 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, „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დადგენის შესახებ“ სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის N 3 ბრძანებით და სამუშაო აღწერილობით, რომელიც მოიცავს:

6.2.1. ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;

6.2.2. ინფორმაციული უსაფრთხოების მართვის სისტემის მინიმალური მოთხოვნების შესრულების კოორდინირება;

6.2.3. ინფორმაციული აქტივებისა და მათი წვდომის აღწერა;

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

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

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

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

6.2.8. სამოქმედო გეგმის შედგენა და ამ გეგმის შესრულების ყოველწლიური ანგარიშის ზემოთ აღნიშნული ბრძანების მე-4 მუხლის პირველი პუნქტით განსაზღვრული პირებისთვის და სსიპ ციფრული მმართველობის 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.

6.2.10. ინფორმაციული უსაფრთხოების აუდიტის პროცესის ხელშეწყობა.

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

7. მესამე მხარეები

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

8. აქტივების მართვა

8.1. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი 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. ბათუმის საერთაშორისო საკონტეინერო ტერმინალის 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.

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. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი 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. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი უზრუნველყოფს ინციდენტების შესახებ დაინტერესებულ მხარეებთან კომუნიკაციას კანონით დადგენილი წესების შესაბამისად.

14. ბიზნეს უწყვეტობის მართვა

14.1. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი შეიმუშავებს უწყვეტობის გეგმებს, რომელიც საშუალებას მისცემს ორგანიზაცის 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. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი 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. გამოვლენილი შეუსაბამობების აღმოსაფხვრელად, ორგანიზაცია მოამზადებს გეგმას და უზრუნველყოფს აღმოფხვრის პროცესის ეფექტიან განხორციელებას.

16. ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

16.1. ბათუმის საერთაშორისო საკონტეინერო ტერმინალი 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.

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.

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.