ინფორმაციული უსაფრთხოების პოლიტიკა

დოკუმენტის კონტროლი

დოკუმენტის სახელი	ინფორმაციული უსაფრთხოების პოლიტიკა
დოკუმენტის მფლობელი	ინფორმაციული უსაფრთხოების მენეჯერი
კლასიფიკატორი	საჯარო/Public
დოკუმენტის განხილვა	ინფორმაციული უსაფრთხოების საბჭო
დოკუმენტის დამტკიცება	გენერალური დირექტორი
დოკუმენტის თარიღი	05.03.2026
დოკუმენტის ნომერი	03-01
დოკუმენტის ვერსია	5.0

დოკუმენტის ისტორია

ვერსია	ცვლილების მოკლე აღწერა	ცვლილების თარიღი
1.0	დოკუმენტის საწყისი ვერსიის დამტკიცება	12.09.2023
2.0	განახლებულია მარეგულირებლის რეკომენდაციების შესაბამისად	22.11.2023
3.0	დოკუმენტის ყოველწლიური განახლება	30.12.2024
4.0	დოკუმენტის ყოველწლიური განახლება	29.12.2025
5.0	დოკუმენტის სტრუქტურის და ფორმატის ცვლილება	05.03.2026

სარჩევი

ინფორმაციული უსაფრთხოების პოლიტიკა

1. შინაარსი

1.1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის თანახმად დარეგულირებულია კრიტიკული ინფორმაციის სისტემის სუბიექტების სამი კატეგორია. კანონის მიხედვით მესამე კატეგორიის კრიტიკული ინფორმაციის სისტემის სუბიექტს წარმოადგენს სადაზღვევო სექტორის ორგანიზაციები. საქართველოს მთავრობის 2021 წლის 31 დეკემბრის N646 დადგენილებით სადაზღვევო კომპანია ალდაგი წარმოადგენს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტს.

1.2. ორგანიზაციის მისიისა და მიზნების ეფექტიანად განხორციელებისთვის ალდაგისთვის მნიშვნელოვანია ორგანიზაციის ინფორმაციული აქტივების უსაფრთხოების უზრუნველყოფა და სათანადო დონეზე დაცვა (კონფიდენციალობა, ხელმისაწვდომობა და მთლიანობა).

1.3. სადაზღვევო კომპანია ალდაგი ინფორმაციული უსაფრთხოების პოლიტიკა აღწერს ინფორმაციული უსაფრთხოების მართვის სისტემის ფუნქციონირების ძირითად პრინციპებს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის, სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ N1 ბრძანების და ISO/IEC 27001:2022 სტანდარტის მოთხოვნების შესაბამისად.

1.4. მოცემული დოკუმენტი არის ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში–იუმს) დოკუმენტაციის განუყოფელი ნაწილი.

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 (იუმს)** - 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. **რისკის ანალიზი** - ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მისი შეფასების დასადგენად;
2.8. **რისკების მართვა** - ორგანიზაციის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;
2.9. **რისკების მოპყრობა** - რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

3. ინფორმაციული უსაფრთხოების პოლიტიკის მიზანი

ინფორმაციული უსაფრთხოების პოლიტიკის მიზანია ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის წესების და ძირითადი მიდგომების დადგენა.

4. ინფორმაციული უსაფრთხოების ამოცანები

ინფორმაციული უსაფრთხოების ამოცანებია:

4.1. ინფორმაციული უსაფრთხოების სფეროში საკანონდებლო, სახელშეკრულებო და მარეგულირებელ მოთხოვნებთან შესაბამისობის უზრუნველყოფა.
4.2. ინფორმაციული უსაფრთხოების მართვის სისტემის გაუმჯობესება, შესაბამისობის მიღწევა და სერტიფიცირება ISO 27001:2022 სტანდარტით.
4.3. ინფორმაციული უსაფრთხოების რისკების შეფასებისა და რისკების მოპყრობის გეგმის საფუძველზე შეიძლება განისაზღვროს დამატებითი ამოცანები.

5. პოლიტიკის მოქმედების სფერო

5.1. ინფორმაციული უსაფრთხოების პოლიტიკა ვრცელდება სადაზღვევო კომპანია ალდაგის:
  5.1.1. ყველა თანამშრომელზე;
  5.1.2. ყველა ბიზნეს პროცესზე (ძირითადი და მხარდამჭერი პროცესები);
  5.1.3. ყველა ტიპის ინფორმაციულ აქტივზე;
  5.1.4. მესამე პირებზე, რომელთაც წვდომა აქვთ ალდაგის ინფორმაციულ აქტივებზე ან მონაწილეობენ მათ დამუშავებაში.
5.2. მოქმედების სფეროს კომპონენტები დაზუსტებულია ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტში.

6. ინფორმაციული უსაფრთხოების საბჭო

6.1. სადაზღვევო კომპანია ალდაგი ორგანიზაციში ქმნის სათათბირო ორგანოს - ინფორმაციული უსაფრთხოების საბჭოს, რომლის მიზანია ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანი ფუნქციონირება და შესაბამისობა.

6.2. ინფორმაციული უსაფრთხოების საბჭოში წარმოდგენილია:

6.2.1. ორგანიზაციის მენეჯმენტი;

6.2.2. ძირითადი ბიზნეს პროცესების მფლობელი სტრუქტურული ერთეულის ხელმძღვანელები;

6.2.3. მხარდამჭერი ბიზნეს პროცესების მფლობელი სტრუქტურული ერთეულის ხელმძღვანელები;

6.2.4. ინფორმაციული უსაფრთხოების მენეჯერი.

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

7. ინფორმაციული უსაფრთხოების მენეჯერი

7.1. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია ინფორმაციული უსაფრთხოების საბჭოსთან;

7.2. ინფორმაციული უსაფრთხოების მენეჯერის ვალდებულებები და ფუნქციები განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-7 მუხლში და დარეგულირებულია ალდაგის სამუშაო აღწერილობით.

8. მესამე მხარეები

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

9. ინფორმაციული აქტივების მართვა

9.1. სადაზღვევო კომაპნია ალდაგი უზრუნველყოფს ინფორმაციული აქტივების იდენტიფიკაციას და კლასიფიკაციას, ასევე მათი შეცვლის, მართვის და განადგურების წესების დადგენას.

9.2. ინფორმაციული აქტივების იდენტიფიცირებისა და კლასიფიკაციის წესები განსაზღვრულია ალდაგის ინფორმაციული აქტივების იდენტიფიცირების მეთოდოლოგიაში და ინფორმაციული აქტივების კლასიფიკაციის მეთოდოლოგიაში.

10. რისკების მართვა

10.1. სადაზღვევო კომპანია ალდაგი ინფორმაციული უსაფრთხოების მართვის სისტემა დაფუძნებულია ინფორმაციული უსაფრთხოების რისკების მართვის პროცესზე, პროცესის ფარგლებში კომპანია:

10.1.1. განსაზღვრავს ინფორმაციული უსაფრთხოების რიკების იდენტიფიცირებისა და შეფასების მიდგომებს;

10.1.2. ავლენს ინფორმაციული უსაფრთხოების რისკებს, აანალიზებს მათ გავლენას და ატარებს რისკების ანალიზს;

10.1.3. რისკების მოპყრობის მიზნით არჩევს საჭირო კონტროლის მექანიზმებს და განსაზღვრავს მისაღები რისკის დონეს.

10.1.4. ამზადებს რისკების მოპყრობის გეგმას.

10.2. რისკების შეფასების და მართვის პროცესის დეტალები მოცემულია ინფორმაციული უსაფრთხოების რისკების მართვის მეთოდოლოგიაში.

11. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

11.1. სადაზღვევო კომპანია ალდაგი ადგენს კონტროლის მექანიზმების გამოყენებადობის განაცხადს, რომელიც შეიცავს:

11.1.1. ინფორმაციული უსაფრთხოების მოთხოვნებისთვის შერჩეულ კონტროლის მიზნებს და კონტროლის მექანიზმებს, ასევე მათი შერჩევის დასაბუთებას;

11.1.2. კომპანიაში უკვე დანერგილი კონტროლის მიზნებს და კონტროლის მექანიზმებს;

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

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

11.3. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნების მისაღწევად ალდაგი:

11.3.1. ნერგავს შერჩეულ კონტროლის მექანიზმებს;

11.3.2. კონტროლის მექანიზმების დანერგვის შემდგომ აწარმოებს მათზე დაკვირვებას;

11.3.3. აანალიზებს დაკვირვების შედეგებს და საჭიროების შემთხვევაში განსაზღრავს სამოქმედო გეგმას.

12. ინფორმაციული უსაფრთხოების ინციდენტების მართვა

12.1. სადაზღვევო კომპანია ალდაგი უზრუნველყოფს ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცესის ეფექტიან განხორციელებას;

12.2. ინფორმაციული უსაფრთხოების ყველა ინციდენტი აღირიცხება და მუშავდება ალდაგის ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცედურის შესაბამისად.

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

13. ბიზნეს უწყვეტობის მართვა

13.1. სადაზღვევო კომპანია ალდაგი უზრუნველყოფს ბიზნეს უწყვეტობის ეფექტურ განხირციელეებას, რომელიც საშუალებას მისცემს ორგანიზაციას ფორსმაჟორის დროს აღადგინოს ყველა საჭირო სერვისი დროის მოკლე მონაკვეთში.

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

14. ინფორმაციულ სისტემაში შეღწევადობის ტესტი

14.1. სადაზღვევო კომპანია ალდაგი უზრუნველყოფს ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროში შემავალ ყველა კრიტიკულ ინფორმაციულ სისტემაზე შეღწევადობის ტესტის ჩატარებას, წინასწარ დაგეგმილი ვადებით და დოკუმენტირებული ამოცანის მიხედვით.

14.2. შეღწევადობის ტესტის შედეგად გამოვლენილი სისუსტეების აღმოსაფხვრელად, ალდაგი ამზადებს სამოქმედო გეგმას და უზრუნველყოფს აღმოფხვრის პროცესის ეფექტიან აღსრულებას.

15. ინტელექტუალური საკუთრების დაცვა

სადაზღვევო კომპანია ალდაგი იცავს ინტელექტუალური საკუთრების უფლებებს - საკუთარ ტექნოლოგიურ გარემოში იყენებს, მხოლოდ ლიცენზირებულ პროგრამულ უზრუნველყოფებს და გადაწყვეტილებებს, მათ შორის ღია კოდის (Open Source) პროდუქტებს, მწარმოებლის მიერ დადგენილი ლიცენზიის პირობების დაცვით.

16. ცნობიერების ამაღლება და კომპეტენციების განვითარება

16.1. ორგანიზაცია განახორციელებს ინფორმაციული უსაფრთხოების ცნობიერების ამაღლების პროგრამებს, ასევე მუდმივად ზრუნავს თანამშრომელთა კომპეტენციების განვითარებაზე.

16.2. ცნობიერების ამაღლების და კომპეტენციების განვითარების მიმართულებით, ალდაგი:

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

16.2.2. უზრუნველყოფს ტრენინგებს და სხვადასხვა აქტივობებს ინფორმაციული უსაფრთხოების მოთხოვნების დასაკმაყოფილებლად;

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

16.2.4. აფასებს პერსონალის ცოდნის და ცნობიერების დონეს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელობაზე.

17. ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტების მართვა

17.1. სადაზღვევო კომპანია ალდაგი ზრუნავს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის უახლესი ვერსიის ხელმისაწვდომობას ყველა დაინტერესებული პირისთვის, ასევე უზრუნველყოფს მართვის სისტემის დოკუმენტაციის სათანადოდ დაცვასა და კონტროლს.

17.2. ალდაგი ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლებში აწარმოებს სათანადო ჩანაწერებს და უზრუნველყოფს მათ მხარდაჭერას მართვის სისტემის მოთხოვნების შესაბამისად. მართვის სისტემის ფუნქციონირების ფარგლებში შემუშავებული ჩანაწერები სათანადოდ არის დაცულია და მართული.

18. ინფორმაციული უსაფრთხოების მართვის სისტემის შიდა აუდიტი

18.1. სადაზღვევო კომპანია ალდაგი დადგენილი პერიოდულობით ატარებს ინფორმაციული უსაფრთხოების მართვის სისტემის აუდიტს და დაადგენს სისტემის შესაბამისობას:

18.1.1. საკანონმდებლო და სტანდარტის მოთხოვნებთან;

18.1.2. უსაფრთხოების მოთხოვნებთან.

18.2. გამოვლენილი შეუსაბამობების აღმოსაფხვრელად, ალდაგი ამზადებს გეგმას და უზრუნველყოფს მაკორექტირებელი აქტივობების ეფექტიან განხორციელებას.

19. ხელმძღვანელობის მიერ იუმს-ის განხილვა

19.1. ალდაგის მაღალი რგოლის მენეჯმენტი, ინფორმაციული უსაფრთხოების საბჭოს ფორმატში, არანაკლებ წელიწადში ორჯერ უზრუნველყოფს იუმს-ის განხილვას,

რათა უზრუნველყოფილი იყო მისი მუდმივი შესაბამისობა, ადეკვატურობა და ეფექტიანობა, მათ შორის:

19.1.1. წინა განხილვის შემდგომ განხორციელებულ ღონისძიებათა სტატუსი;

19.1.2. ორგანიზაციული კონტექსტის და გარე ფაქტორების ცვლილებები, რომლებმაც შესაძლოა გავლენა იქონიონ ინფორმაციული უსაფრთხოების მართვის სისტემაზე;

19.1.3. უკუკავშირი ინფორმაციული უსაფრთხოების წარმადობასთან დაკავშირებით, მათ შორის:

19.1.3.1. უკუკავშირი დაინტერესებული მხარეებისგან;

19.1.3.2. რისკების შეფასების შედეგები და რისკებთან მოპყრობის გეგმის სტატუსი;

19.1.3.3. ახალი შესაძლებლობები გაუმჯობესებისთვის.

20. მუდმივი გაუმჯობესება

სადაზღვევო კომპანია ალდაგის ამ პოლიტიკით დადგენილი ინსტრუმენტების გამოყენებით უზრუნველყოფს ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისობის, ადეკვატურობის და ეფექტიანობის მუდმივი გაუმჯობესების ციკლს.

21. პოლიტიკის გადახედვის გეგმა

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

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

22. დაკავშირებული დოკუმენტები

ინფორმაციული უსაფრთხოების პოლიტიკა დაკავშირებულია შემდეგ დოკუმენტებთან:

22.1. ინფორმაციული უსაფრთხოების საბჭოს დებულება;

22.2. ორგანიზაციული კონტექსტის დოკუმენტი;

22.3. ინფორმაციული უსაფრთხოების გავრცელების სფეროს დოკუმენტი.