საჯარო სამართლის იურიდიული პირის - სახელმწიფო სერვისების განვითარების სააგენტოს ინფორმაციული უსაფრთხოების პოლიტიკა

თავი I
ზოგადი დებულებები

მუხლი 1. შესავალი

1. საჯარო სამართლის იურიდიული პირის - სახელმწიფო სერვისების განვითარების სააგენტოს (შემდგომ - სააგენტო) ინფორმაციული უსაფრთხოების პოლიტიკა შემუშავებულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და ISO 27001:2022 ინფორმაციული უსაფრთხოების სტანდარტის მოთხოვნების შესაბამისად.

2. ინფორმაციული უსაფრთხოების პოლიტიკა არის ინფორმაციული უსაფრთხოების მართვის სისტემის მთავარი დოკუმენტი. სააგენტოს თავმჯდომარის ბრძანებით დამტკიცებული ინფორმაციული უსაფრთხოების სხვა სტანდარტები უნდა შეესაბამებოდეს ინფორმაციული უსაფრთხოების პოლიტიკას.

მუხლი 2. ტერმინთა განმარტება

ინფორმაციული უსაფრთხოების პოლიტიკის მიზნებისათვის მასში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) ინფორმაციული უსაფრთხოება - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციის კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობის შენარჩუნებას და დაცვას.

ბ) ხელმისაწვდომობა - ავტორიზებული სუბიექტის მოთხოვნის შესაბამისად ინფორმაციულ აქტივზე წვდომის და გამოყენების მახასიათებელი;

გ) კონფიდენციალურობა - ინფორმაციული აქტივის მახასიათებელი, რომლის თანახმადაც, ინფორმაციული აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული ინდივიდების, სუბიექტების ან პროცესებისათვის;

დ) მთლიანობა - ინფორმაციული აქტივის სიზუსტის და სისრულის მახასიათებელი;

ე) ინფორმაციული უსაფრთხოების ინციდენტი - ინფორმაციული უსაფრთხოების მოულოდნელი ან არასასურველი, ცალკეული ან სერიული ხდომილებები, რომლებიც, დიდი ალბათობით, ახდენენ ბიზნესოპერაციების დისკრედიტაციას, ან ემუქრებიან ინფორმაციულ უსაფრთხოებას;

ვ) პოლიტიკა - სააგენტოს თავმჯდომარის ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტით დამტკიცებული სააგენტოს მიზნები და მიმართულებები; ამ ბრძანებით, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება სააგენტოს ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს;

ზ) რისკი - მოვლენისა და მისი უარყოფითი შედეგების ალბათობის კომბინაცია;

თ) კონტროლის მექანიზმი - რისკების მართვის საშუალება, მათ შორის, პოლიტიკა, პროცედურები, სახელმძღვანელო მითითებები ან ორგანიზაციული სტრუქტურები, რომლებიც შეიძლება იყოს ადმინისტრაციული, ტექნიკური, მმართველობითი ან იურიდიული ხასიათის;

ი) მესამე მხარე - ფიზიკური ან იურიდიული პირი, სტრუქტურული ერთეული/ქვედანაყოფი ან ტერიტორიული სამსახური, რომელიც მოიაზრება, როგორც პროცესში ჩართული მხარეებისგან დამოუკიდებელი სუბიექტი;

კ) საფრთხე - არასასურველი მოვლენის პოტენციური მიზეზი, რამაც შეიძლება დააზიანოს სისტემა ან ორგანიზაცია;

ლ) სისუსტე - ინფორმაციული აქტივის ან ინფორმაციულ აქტივთა ჯგუფისთვის დამახასიათებელი ნაკლი, რომელიც შეიძლება იყოს საფრთხის შემცველი;

მ) რისკის მიღება - გადაწყვეტილება რისკის დასაშვებად მიჩნევის თაობაზე;

ნ) ინფორმაციული უსაფრთხოების მართვის სისტემა - სააგენტოს მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

ო) ინფორმაციული აქტივი – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სააგენტოსთვის.

პ) ინფორმაციული აქტივების მართვა - ინფორმაციული აქტივების აღწერა, კლასიფიცირება, წვდომა, შეცვლა, განადგურება.

მუხლი 3. სააგენტოს ინფორმაციული უსაფრთხოების პოლიტიკის მიზნები

1. ინფორმაციული უსაფრთხოების პოლიტიკის მიზანი არის სააგენტოს პროდუქტების ხარისხის განვითარება, ბიზნესპროცესების უწყვეტობის ხელშეწყობა, ბიზნესრისკების შემცირება, ფინანსური რესურსების ეფექტურად მართვა და საქმიანობის კანონმდებლობასთან შესაბამისობის უზრუნველყოფა.

2. ინფორმაციული უსაფრთხოების პოლიტიკის მიზნების მისაღწევად სააგენტოში ინერგება ISO 27001:2022 ინფორმაციული უსაფრთხოების სტანდარტთან თავსებადი ინფორმაციული უსაფრთხოების მართვის სისტემა.

3. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვას რისკების მართვის პროცესის გამოყენებით და, ამავდროულად, ზრდის დაინტერესებული მხარეების ნდობას სააგენტოს მიერ მიწოდებული სერვისებისადმი;

მუხლი 4. ინფორმაციული უსაფრთხოების პოლიტიკის პრინციპები

1. ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი პრინციპია ინფორმაციის საფრთხეებისაგან დაცვა, რათა უზრუნველყოფილი იყოს ბიზნესპროცესების უწყვეტობა, რისკების შემცირება, პრევენციული ქმედებების განხორციელებით საფრთხის პოტენციური უარყოფითი გავლენის შემცირება, ინფორმაციისა და ინფორმაციული სისტემების კონფიდენციალურობის, მთლიანობისა და განგრძობადი მუშაობის დაცვა.

2. სააგენტოს ინფორმაციული უსაფრთხოება მიიღწევა შესაბამისი კონტროლის მექანიზმების, მათ შორის, პოლიტიკების, პროცესების, პროცედურების, ორგანიზაციული სტრუქტურისა და პროგრამული უზრუნველყოფის, აგრეთვე ინფორმაციული ტექნოლოგიების დანერგვით. სააგენტომ უნდა ჩამოაყალიბოს, დანერგოს კონტროლის

მექანიზმები, აწარმოოს მათი მონიტორინგი და, საჭიროების შემთხვევაში, გააუმჯობესოს, რათა უზრუნველყოს სააგენტოს მიზნების მიღწევა და დაცვა.

მუხლი 5. ინფორმაციული უსაფრთხოების პოლიტიკის გავრცელების სფერო

ინფორმაციული უსაფრთხოების პოლიტიკა ვრცელდება ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტით დადგენილ ბიზნესპროცესებზე და სავალდებულოა შესასრულებლად მათ ფარგლებში იდენტიფიცირებულ ყველა ინფორმაციულ აქტივზე.

მუხლი 6. ინფორმაციული უსაფრთხოების პოლიტიკის ამოცანები

ინფორმაციული უსაფრთხოების პოლიტიკის ამოცანებია:

ა) ინფორმაციული აქტივების მართვა;

ბ) ადამიანური რესურსების უსაფრთხოება;

გ) ფიზიკური და გარემოს უსაფრთხოება;

დ) კომუნიკაციებისა და ოპერაციების მართვა;

ე) ინფორმაციულ აქტივებზე წვდომის კონტროლი;

ვ) ინფორმაციული სისტემების შეძენა, შემუშავება და მხარდაჭერა;

ზ) ინფორმაციული უსაფრთხოების ინციდენტების მართვა;

თ) ბიზნესპროცესების უწყვეტობის მართვა;

ი) შესაბამისობა.

მუხლი 7. ინფორმაციული უსაფრთხოების პოლიტიკის სუბიექტები

ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნები ვრცელდება შემდეგ სუბიექტებზე:

ა) სააგენტოს თანამშრომელზე;

ბ) პირზე, რომელიც სტაჟირებას გადის სააგენტოში;

გ) პირზე, რომელსაც სხვა საფუძვლით დაშვება აქვს სააგენტოს ინფორმაციულ აქტივებზე.

თავი II
ინფორმაციული უსაფრთხოების მართვის სისტემის ორგანიზება

მუხლი 8. სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს ინფორმაციული უსაფრთხოების საბჭო

1. სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს ინფორმაციული უსაფრთხოების საბჭო (შემდგომ - ინფორმაციული უსაფრთხოების საბჭო), სხვა ფუნქციებთან ერთად, პასუხისმგებელია სააგენტოს ხელმძღვანელობის მიერ ინფორმაციული უსაფრთხოების სფეროში დასახული მიზნების მიღწევაზე.

2. ინფორმაციული უსაფრთხოების საბჭოს როლი და პასუხისმგებლობა განისაზღვრება ინფორმაციული უსაფრთხოების საბჭოს დებულებით.

მუხლი 9. ინფორმაციული უსაფრთხოების მენეჯერი

1. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია სააგენტოს თავმჯდომარისა და ინფორმაციული უსაფრთხოების საბჭოს წინაშე, ასევე ყოველწლიურ ანგარიშს წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს. ინფორმაციული უსაფრთხოების

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

2. ინფორმაციული უსაფრთხოების მენეჯერის მოვალეობები განსაზღვრულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით და სააგენტოს თავმჯდომარის სამართლებრივი აქტებით.

მუხლი 10. ინფორმაციული უსაფრთხოების აუდიტი

1. ინფორმაციული უსაფრთხოების აუდიტის მიზანია ინფორმაციული უსაფრთხოების მართვის სისტემის „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონთან და ISO 27001:2022 სტანდარტთან შესაბამისობის პერიოდული შემოწმება.

2. ინფორმაციული უსაფრთხოების მართვის სისტემის პირველად აუდიტს ატარებს საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირი - ოპერატიულ-ტექნიკური სააგენტო (შემდგომ - ოპერატიულ-ტექნიკური სააგენტო). შემდგომ ინფორმაციული უსაფრთხოების პერიოდულ აუდიტს სააგენტოს შერჩევით ატარებს ოპერატიულ-ტექნიკური სააგენტო ან საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის - ციფრული მმართველობის სააგენტოს (შემდგომ - ციფრული სააგენტო) მიერ ავტორიზებული ორგანიზაცია.

3. ინფორმაციული უსაფრთხოების აუდიტის ჩატარების შემდეგ დგება აუდიტის დასკვნა, რომლის მოთხოვნების შესრულება სავალდებულოა. ინფორმაციული უსაფრთხოების აუდიტის ციფრული მმართველობის სააგენტოს მიერ ავტორიზებული ორგანიზაციის მიერ ჩატარების შემთხვევაში, აღნიშნული აუდიტის დასკვნის 1 ეგზემპლარს აუდიტის დასრულებისთანავე სააგენტო წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს.

მუხლი 11. ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი

1. ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტი ტარდება წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით. აღნიშნული ტესტის ჩატარების შემდეგ დგება პენეტრაციის ტესტის დასკვნა, რომლითაც სრულდება ტესტი და რომლის მოთხოვნების შესრულება სავალდებულოა. პენეტრაციის ტესტს ატარებს ოპერატიულ-ტექნიკური სააგენტო. ინფორმაციულ სისტემაში შეღწევადობის ტესტი ტარდება მინიმუმ 3 წელიწადში ერთხელ, გარდა იმ შემთხვევისა, როდესაც ტესტის ჩატარების თარიღი ემთხვევა სააგენტოს პენეტრაციის ტესტს დაქვემდებარებული საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის, მათ შორის, პროგრამული უზრუნველყოფის პროგრამების განახლების ან/და დამატებითი კონტროლის დანერგვის პერიოდს. ასეთ შემთხვევაში პენეტრაციის ტესტი ტარდება ინფრასტრუქტურის განახლების ან/და დამატებითი კონტროლის დანერგვიდან არაუგვიანეს 2 თვის ვადაში.

2. თუ პენეტრაციის ტესტის ჩატარების შედეგად აღმოჩენილი იქნება ინფორმაციული სისტემის სისუსტეები, სააგენტო ატარებს ამ შეუსაბამობების/სისუსტეების ანალიზს და მათ აღმოსაფხვრელად განსაზღვრავს სამოქმედო გეგმას, რომელიც უნდა შეიცავდეს მისი შესრულების გრაფიკს. სამოქმედო გეგმას პენეტრაციის ტესტის დასრულებიდან 1 თვის ვადაში სააგენტო წარუდგენს ოპერატიულ-ტექნიკურ სააგენტოს.

თავი III
ინფორმაციული უსაფრთხოების მართვის სისტემის კომპონენტები

მუხლი 12. ინფორმაციული აქტივების მართვა

1. ინფორმაციული აქტივების მართვის მიზნით სააგენტო ახორციელებს ინფორმაციული აქტივების აღწერას და კლასიფიცირებას მათი გამოყენების წესებისა და სათანადო დაცვის ხარისხის მითითებით.

2. ყოველ ინფორმაციულ აქტივს გააჩნია მასზე პასუხისმგებელი პირი ან სტრუქტურული ერთეული - ინფორმაციული აქტივის მფლობელი.

3. ინფორმაციული აქტივების გამოყენების წესები განისაზღვრება სააგენტოს თავმჯდომარის ბრძანებით.

მუხლი 13. ადამიანური რესურსების მართვა

1. ადამიანური ფაქტორით გამოწვეული შეცდომებისა და განზრახ ჩადენილი საზიანო ქმედების იდენტიფიცირებისა და მათი შემცირების მიზნით, სააგენტო ნერგავს შესაბამისი კონტროლის მექანიზმებს.

2. თანამშრომელთა შერჩევა-დაქირავების პროცესში სააგენტო ითვალისწინებს ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნებს.

3. ინფორმაციული უსაფრთხოების მართვის სისტემის სუბიექტების ცნობიერების ამაღლების, მათ შორის, ინფორმაციული უსაფრთხოების მართვის სისტემაში მათი როლისა და პასუხისმგებლობის გაცნობიერების მიზნით, სააგენტო უზრუნველყოფს შესაბამისი ტრენინგების ჩატარებას.

მუხლი 14. ფიზიკური და გარემოს უსაფრთხოება

1. ფიზიკური უსაფრთხოების სათანადო დონის უზრუნველსაყოფად სააგენტო შეიმუშავებს ფიზიკური წვდომის კონტროლის მექანიზმებს.

2. ფიზიკური წვდომის კონტროლის მექანიზმები გულისხმობს ინფორმაციის დამუშავების საშუალებათა უსაფრთხო/დაცულ ზონაში განთავსებას, უსაფრთხოების პერიმეტრებისა და ბარიერების მოწყობას.

3. სააგენტო შეიმუშავებს ფიზიკური წვდომის კონტროლის მექანიზმებს ინფორმაციული ტექნოლოგიების იმ კომპონენტებზე, რომლებიც დაკავშირებულია მონაცემთა დამუშავებისა და შენახვის საშუალებებთან.

მუხლი 15. საკომუნიკაციო და საოპერაციო მართვა

ინფორმაციის დამუშავების ყველა საშუალების სათანადოდ ფუნქციონირება და მართვა უზრუნველყოფილია შესაბამისი უფლება-მოვალეობების გამიჯვნით და პროცედურების შემუშავებით, რათა შემცირდეს საკომუნიკაციო და საოპერაციო სისტემების განზრახ ან შემთხვევით არასწორად გამოყენების რისკი.

მუხლი 16. წვდომის კონტროლი

1. სააგენტო აღრიცხავს კლასიფიცირებულ ინფორმაციულ აქტივებზე წვდომის ფაქტებს. ამ მიზნით სააგენტო იყენებს უფლებების მართვის სისტემებს როგორც ინფორმაციული ტექნოლოგიების საშუალებების გამოყენების, ასევე ინფორმაციული აქტივების ფიზიკური ხელმისაწვდომობის შემთხვევებში.

2. ინფორმაციული აქტივების არასანქცირებული ხელმისაწვდომობის ფაქტების თავიდან აცილების მიზნით, სააგენტო გამოავლენს, შეიმუშავებს და ნერგავს შესაბამისი კონტროლის მექანიზმებს.

3. ინფორმაციაზე, მისი დამუშავების მოწყობილობებსა და ბიზნესპროცესებზე წვდომის კონტროლი ხორციელდება ბიზნესის (საქმიანობის) და უსაფრთხოების მოთხოვნების საფუძველზე.

4. პერსონალური ინფორმაციის ხელმისაწვდომობის წესები და პროცედურები განისაზღვრება სააგენტოს თავმჯდომარის ბრძანებით.

5. წვდომის კონტროლი მოიცავს ინფორმაციული უსაფრთხოების შემდეგ საკითხებს:

ა) წვდომის კონტროლის პოლიტიკას;

ბ) მომხმარებლის წვდომის მართვას;

გ) მომხმარებლის პასუხისმგებლობას;

დ) ქსელთან წვდომის კონტროლს;

ე) ოპერაციულ სისტემასთან წვდომის კონტროლს;

ვ) პროგრამულ უზრუნველყოფასთან და მასში ასახულ ინფორმაციასთან წვდომის კონტროლს;

ზ) მობილურ ტექნოლოგიებს და დისტანციურ მუშაობას.

6. ინფორმაციულ აქტივებზე თანამშრომელთა წვდომის უფლებების მართვა განისაზღვრება მათი უფლება-მოვალეობის შესაბამისად და უზრუნველყოფილია სათანადო კონტროლის მექანიზმების მეშვეობით.

მუხლი 17. ინფორმაციული სისტემების შეძენა, შემუშავება და მხარდაჭერა

1. ინფორმაციული სისტემები მოიცავს საოპერაციო სისტემებს, პროგრამულ უზრუნველყოფებს, მესამე მხარის სტანდარტულ პროდუქტებს, ბიზნესპროცესების მხარდამჭერ ინფორმაციულ სისტემებს, რომლებიც შემუშავებულია სააგენტოს თანამშრომელთა მიერ ან მოწოდებულია მესამე მხარის მიერ.

2. წარმატებული და ეფექტიანი ინფორმაციული სისტემების შექმნის მიზნით, მათი დაგეგმვის ეტაპზე, საპროექტო მოთხოვნების შემუშავებისას გათვალისწინებულ უნდა იქნეს ინფორმაციული უსაფრთხოების მოთხოვნები.

მუხლი 18. ინფორმაციული უსაფრთხოების ინციდენტების მართვა

1. ბიზნესპროცესების უწყვეტობის, საოპერაციო ხარჯების ეფექტურად გამოყენების, ასევე სააგენტოს პროდუქტებისა და მომსახურების ხარისხის გაუმჯობესების ხელშეწყობის მიზნით, სააგენტო ახორციელებს ინფორმაციული უსაფრთხოების ინციდენტების მართვას.

2. სააგენტოს ინციდენტების მართვის სისტემა მოიცავს ინციდენტების იდენტიფიცირების, ანგარიშგების, აგრეთვე რეაგირების პროცედურებსა და საშუალებებს.

მუხლი 19. ბიზნესპროცესების უწყვეტობის მართვა

1. ბიზნესპროცესების უწყვეტობის უზრუნველსაყოფად სააგენტო მუდმივად ახორციელებს ბიზნესპროცესების ფორმალიზებას.

2. სააგენტოში დანერგილია რისკების გამოვლენისა და მათი შეფასების სისტემა. ბიზნესპროცესებში გამოვლენილი რისკების შესაბამისად დანერგილია კონტროლის მექანიზმები, რომელთა ეფექტურობის პერიოდული შემოწმება სავალდებულო და აუცილებელია.

3. სააგენტომ უნდა განახორციელოს ბიზნესპროცესების შედეგად მიღებული პროდუქტების ან შექმნილი მონაცემების ხარისხის მუდმივი კონტროლი.

4. პროცესების შეფერხების თავიდან აცილების და რისკების მინიმუმამდე დაყვანის მიზნით სააგენტო შეიმუშავებს ბიზნესუწყვეტობის სტრატეგიას.

5. სააგენტო ბიზნესპროცესების უწყვეტობის უზრუნველსაყოფად ითვალისწინებს ინფორმაციული უსაფრთხოების მოთხოვნებს, აფასებს რისკებს, შეიმუშავებს და ნერგავს საქმიანობის უწყვეტობის გეგმას, ახორციელებს საქმიანობის უწყვეტობის გეგმების ტესტირებას, მხარდაჭერასა და განახლებას.

მუხლი 20. შესაბამისობა

1. შესაბამისობის უზრუნველყოფა გულისხმობს ბიზნესპროცესების:

ა) სააგენტოს საქმიანობის მომწესრიგებელ სამართლებრივ ნორმებთან შესაბამისობას;

ბ) მესამე პირებთან დადებულ სახელშეკრულებო ურთიერთობებთან შესაბამისობას;

გ) ინფორმაციული უსაფრთხოების კანონმდებლობასა და სტანდარტებთან შესაბამისობას.

2. ამ მუხლის პირველი პუნქტით განსაზღვრული ამოცანების შესრულების ხელშეწყობის მიზნით, სააგენტო შეიმუშავებს შესაბამისობის დადგენის პროცედურებს.

თავი IV
დასკვნითი დებულებები

მუხლი 21. ინფორმაციული უსაფრთხოების პოლიტიკის დამტკიცება, გადახედვა და ხელმისაწვდომობა

1. ინფორმაციული უსაფრთხოების პოლიტიკას და მასში ინიციირებულ ცვლილებას, სააგენტოს ინფორმაციული უსაფრთხოების საბჭოს მიერ დამტკიცების შემდგომ, მიიღებს სააგენტოს მმართველი საბჭო და ამტკიცებს სააგენტოს თავმჯდომარე.

2. ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანობის და კანონმდებლობასთან შესაბამისობის უზრუნველყოფის მიზნით, ინფორმაციული უსაფრთხოების პოლიტიკა ექვემდებარება პერიოდულ განხილვას/გადახედვას ინფორმაციული უსაფრთხოების საბჭოს მიერ და, საჭიროების შემთხვევაში, ცვლილებების ინიციირებას. აღნიშნული არ გამორიცხავს ინფორმაციული უსაფრთხოების პოლიტიკის ან ამ მუხლის მე-3 პუნქტით განსაზღვრული დოკუმენტების სხვა დროს გადახედვის და ცვლილებების შეტანის შესაძლებლობებს.

3. წელიწადში ერთხელ სავალდებულო განხილვა/გადახედვას და, საჭიროების შემთხვევაში, ცვლილებების შეტანას ექვემდებარება ინფორმაციული უსაფრთხოების მართვასთან დაკავშირებული შემდეგი დოკუმენტები:

ა) ინფორმაციული აქტივების იდენტიფიკაციის მეთოდოლოგია;

ბ) რისკების მართვის მეთოდოლოგია.

4. ინფორმაციული უსაფრთხოების პოლიტიკა, ასევე, მასში შეტანილი ცვლილება ვებგვერდებზე - ID.ge და sda.gov.ge - განთავსდება დამტკიცებიდან არაუგვიანეს 5 სამუშაო დღის განმავლობაში. მის გამოქვეყნებაზე პასუხისმგებელია სააგენტოს ინფორმაციული უსაფრთხოების მენეჯერი.