პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკა

1. შესავალი

პერსონალურ მონაცემთა დაცვის სამსახური (შემდგომ - სამსახური) არის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის საფუძველზე შექმნილი და მოქმედი დამოუკიდებელი სახელმწიფო ორგანო. პერსონალურ მონაცემთა დაცვის სამსახური საქმიანობის განხორციელებისას ხელმძღვანელობს საქართველოს კონსტიტუციით, საქართველოს საერთაშორისო ხელშეკრულებებით, საერთაშორისო სამართლის საყოველთაოდ აღიარებული პრინციპებითა და ნორმებით, ამ კანონითა და სხვა სათანადო სამართლებრივი აქტებით.

სამსახურის საქმიანობის ძირითადი მიმართულებებია:

- პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი;
- ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი.

სამსახურის საქმიანობის პრინციპებია:

ა) კანონიერება;

ბ) ადამიანის უფლებათა და თავისუფლებათა დაცვა;

გ) დამოუკიდებლობა და პოლიტიკური ნეიტრალიტეტი;

დ) ობიექტურობა და მიუკერძოებლობა;

ე) პროფესიონალიზმი;

ვ) საიდუმლოებისა და კონფიდენციალობის დაცვა.

სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკა (შემდგომ - პოლიტიკა) არის სამსახურში ინფორმაციული უსაფრთხოების სფეროში უპირატესი ძალის მქონე შიდა დოკუმენტი, რომელიც ეყრდნობა საქართველოს კანონმდებლობას, ინფორმაციული უსაფრთხოების სფეროში ფართოდ გავრცელებულ საერთაშორისო სტანდარტებს, რეგულაციებს და უზრუნველყოფს:

ა) ფასეული ინფორმაციის დაცულობას არაავტორიზებული გამჟღავნებისაგან;
ბ) ინფორმაციის სიზუსტეს და გამოყენებას სამსახურის საქმიანობის ღირებულებებისა და მისი ფასეულობების შესაბამისად;
გ) ინფორმაციის ხელმისაწვდომობას მაშინ, როდესაც მას მოითხოვს უფლებამოსილი პირი ან საქმიანი პროცესი.
დ) სამსახურში ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას და წარმოადგენს ინფორმაციული უსაფრთხოების დეტალური სტანდარტების, პროცედურებისა და სახელმძღვანელოების შექმნის საფუძველს.

2. ტერმინთა განმარტება

ამ პოლიტიკის მიზნებისათვის, წინამდებარე დოკუმენტში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) უფლებამოსილი პირი - ავტორიზებული მომხმარებელი (თანამშრომელი, სტაჟიორი, მესამე პირი),

რომელსაც აქვს სანქცირებული წვდომა სამსახურის ინფორმაციულ აქტივსა და სისტემებზე;

ბ) ინფორმაციული უსაფრთხოება - ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა;

გ) ინფორმაციული სისტემა – ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას;

დ) ინფორმაციული აქტივი – ყველა სახის ინფორმაცია, ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ;

ე) ფასეული ინფორმაცია - სამსახურში არსებული სენსიტიური და მნიშვნელოვანი ინფორმაცია, რომელზეც არაავტორიზებული წვდომა ან რომლის გამჟღავნებაც ზიანს მიაყენებს სამსახურს ან/და მის მოსამსახურეებს, ასევე იმ პირს (ფიზიკური, იურიდიული პირი, სახელმწიფო უწყება, საერთაშორისო ორგანიზაცია), რომლის შესახებაც მუშავდება ინფორმაცია;

ვ) კონტროლის მექანიზმი – ოპერაციების განხორციელებაზე შეზღუდვებისა და წესების შესრულების უზრუნველსაყოფად შექმნილი ქმედებებისა და ტექნოლოგიების ერთობლიობა;

ზ) დამმუშავებელი მოწყობილობა - ინფორმაციული და კომუნიკაციური ტექნოლოგიების მოწყობილობა, რომლის მეშვეობითაც ხდება ინფორმაციის შეგროვება, შენახვა, გავრცელება;

თ) კომპიუტერული ინციდენტი – ქმედება, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ან მიზნად ისახავს ინფორმაციის კონფიდენციალობის, მთლიანობის ან ხელმისაწვდომობის დარღვევას.

ი) შინასამსახურებრივი გამოყენების წესები – წინამდებარე პოლიტიკის დოკუმენტი და ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლებში შემუშავებული დოკუმენტაცია (პოლიტიკა, პროცედურები, სახელმძღვანელოები და სხვა ინფორმაციის შემცველი მასალები), რომელიც ემსახურება სამსახურის ინფორმაციული აქტივებისა და ინფორმაციის დამმუშავებელი მოწყობილობების უსაფრთხოებას;

კ) დაინტერესებული მხარე – ნებისმიერი ფიზიკური ან იურიდიული პირი, ადმინისტრაციული ორგანო, რომელმაც შეიძლება გავლენა მოახდინოს სამსახურის გადაწყვეტილებასა და ქმედებაზე, აგრეთვე, რომლის ინტერესზეც შესაძლოა გავლენა იქონიოს სამსახურის გადაწყვეტილებამ ან ქმედებამ;

ლ) ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომ - იუმს) - სამსახურის მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია სამსახურის საქმიანობის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება.

3. პოლიტიკის მიზანი და მოქმედების ფარგლები

3.1. პოლიტიკა ვრცელდება სამსახურის ინფორმაციული აქტივების დამუშავების ყველა პროცესზე[1].

3.2. პოლიტიკა ვრცელდება სამსახურის უფროსზე, სამსახურის უფროსის პირველ მოადგილეზე და სამსახურის უფროსის მოადგილეზე და სამსახურის მოსამსახურეებზე სამსახურის სტაჟიორებზე, შრომითი ხელშეკრულებით დასაქმებულ პირებზე (შემდგომ - თანამშრომელი) და ასევე ყველა იმ მესამე

[1] პოლიტიკა არ ვრცელდება სამსახურის მიერ ინფორმაციის ფარული საგამოძიებო მოქმედებების კონტროლის მიზნით დამუშავების პროცესებზე, მათ შორის გრიფით „სრულიად საიდუმლო“ და „საიდუმლო“ და არასაიდუმლო დოკუმენტების/ინფორმაციის დამუშავებაზე.

პირზე, რომელსაც წვდომა აქვს სამსახურის ინფორმაციულ აქტივებზე (მაგ. კონსულტანტი, გარე აუდიტორი, აგრეთვე ყველა სხვა პირი, რომელსაც მინიჭებული აქვს სამსახურის ინფორმაციასა და ინფორმაციის დამმუშავებელ მოწყობილობაზე წვდომა).

3.3. პოლიტიკა აყალიბებს ძირითად წესებს, როლებსა და პასუხისმგებლობებს, რომელთა თანახმად, სამსახური იცავს საქმიანობის პროცესში დამუშავებული, მათ შორის შენახული, მიღებული და გაცემული ინფორმაციის უსაფრთხოებას სამსახურში არსებული ნებისმიერი სისტემის გამოყენებით.

3.4. პოლიტიკის მიზანია შიდა და გარე საფრთხეების მიმართ ინფორმაციული უსაფრთხოების ადეკვატური დამცავი მექანიზმების, კრიზისული სიტუაციებისა და განზრახ დაზიანებების წინააღმდეგ ქცევის ძირითადი წესების განსაზღვრა.

3.5. პოლიტიკა მიზნად ისახავს სამსახურში არსებული ინფორმაციის, კანონმდებლობით დაკისრებული ფუნქციების შესრულებისა და რეპუტაციის დაცვის კონტროლის მექანიზმების შექმნას და მისი მეშვეობით ინფორმაციის კონფიდენციალობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფას.

4. პოლიტიკის რეგულირების საგანი და სუბიექტები

4.1. პოლიტიკის რეგულირების საგანს, ინფორმაციული უსაფრთხოების თვალსაზრისით, წარმოადგენს სამსახურის საკუთრებაში ან მფლობელობაში არსებული:

ა) ყველა მონაცემი, მათ შორის თანამშრომლის, განმცხადებლის, მონაცემთა დამმუშავებლის/უფლებამოსილი პირის, ინფორმაციის მიმღების, დაინტერესებული მხარის ან სხვა პირის შესახებ ინფორმაცია;

ბ) სამსახურში შექმნილი თუ მიღებული ინფორმაციული აქტივი (მატერიალური და ელექტრონული სახით);

გ) ყველა ინფორმაციული სისტემა;

დ) ინფორმაციულ-ტექნოლოგიური ინფრასტრუქტურა;

ე) ნებისმიერი სხვა ტექნიკური საშუალება, რომელთა მეშვეობითაც ხორციელდება ინფორმაციის შეგროვება, შენახვა, დაცვა, დაშვების უფლების მინიჭება, გადაცემა, მიღება, ასლის გადაღება, გადატანა, წაშლა, განადგურება ან სხვაგვარი დამუშავება.

4.2. პოლიტიკის რეგულირების საგანს, ინფორმაციული უსაფრთხოების თვალსაზრისით, წარმოადგენს სამსახურის ყველა პროცედურა და დოკუმენტი:

ა) რომელიც აწესრიგებს ინფორმაციასთან, ინფორმაციულ ან გამოთვლით სისტემებთან, ინფორმაციულ-ტექნოლოგიურ ინფრასტრუქტურასთან, დოკუმენტებთან და ინფორმაციის ნებისმიერ მატარებლებთან მუშაობის წესს;

ბ) რომელიც არეგულირებს სამსახურის და მის მომხმარებლებს/მოქალაქეებსა და ორგანიზაციებს შორის ინფორმაციული უსაფრთხოების საკითხებს.

4.3. პოლიტიკის რეგულირების სუბიექტებს, ინფორმაციული უსაფრთხოების თვალსაზრისით, წარმოადგენენ სამსახურის თანამშრომლები და მესამე პირები:

ა) რომლებიც ახორციელებენ სამსახურის კუთვნილ ან სამსახურის განკარგულებაში არსებული ინფორმაციის მართვას/დამუშავებას;

ბ) რომლებიც იყენებენ სამსახურის კუთვნილ ან განკარგულებაში მყოფ ინფორმაციულ სისტემებსა და ინფორმაციულ-ტექნოლოგიურ ინფრასტრუქტურას ან ახორციელებენ მის ადმინისტრირებას.

5. პოლიტიკის ძირითადი პრინციპები

სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკისა და მისი შესაბამისი პროცედურების

საფუძველია საქართველოს კანონმდებლობა და ISO 27000 სერიის სტანდარტები, რომლის მიხედვითაც, სამსახურში მუდმივად დაცული უნდა იყოს ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა:

ა) **კონფიდენციალობა** - ფასეულ ინფორმაციაზე წვდომა დაშვებულია მხოლოდ უფლებამოსილი პირისთვის სამსახურის საქმიანობიდან გამომდინარე და დაკისრებული ფუნქციების შესასრულებლად.

ბ) **მთლიანობა** - მახასიათებელი იმისა, რომ ინფორმაცია არის სწორი, არ არის შეცვლილი განზრახ ან უნებლიედ და ზუსტ ფაქტებს ასახავს. ასევე ინფორმაციული სისტემები და სხვა აქტივები ფუნქციონირებს გამართულად, თავისი დანიშნულების შესაბამისად.

გ) **ხელმისაწვდომობა** - სამსახურის საქმიანობიდან გამომდინარე, ინფორმაცია ხელმისაწვდომი და გამოყენებადია საჭიროებისამებრ, ნებისმიერ დროს, დაკისრებული ფუნქციების შესასრულებლად.

6. ვალდებულებები

6.1. ინფორმაციული უსაფრთხოების წარმატებული და ეფექტიანი სისტემის ჩამოყალიბებისათვის, მართვისა და შემდგომი განვითარებისათვის, საჭიროა სამსახურის მმართველი რგოლის, თანამშრომლებისა და მესამე პირების შეთანხმებული და მიზანმიმართული მუშაობა. აღნიშნული პირები ვალდებულნი არიან, დაიცვან პოლიტიკის მოთხოვნები და აიღონ პასუხისმგებლობა მათთვის დაწესებული სტანდარტებისა და წესების სრულყოფილად და ზედმიწევნით შესრულებაზე.

6.2. ინფორმაციის თითოეულ მომხმარებელს გააჩნია შესაბამისი როლი და პასუხისმგებლობა სამსახურის ინფორმაციული უსაფრთხოების უზრუნველსაყოფად. ყველა თანამშრომელი თუ მესამე პირი/მისი წარმომადგენელი, ვალდებულია, გაითვალისწინოს ინფორმაციული უსაფრთხოების მოთხოვნები, იმოქმედოს პასუხისმგებლობით და მოახდინოს აღმოჩენილი უსაფრთხოების დარღვევების შეტყობინება და ამ მიზნით:

ა) იცოდეს, ესმოდეს და იმოქმედოს იმ პასუხისმგებლობების შესაბამისად, რომლებიც მინიჭებული აქვთ ინფორმაციული უსაფრთხოების პოლიტიკით, სტანდარტებით, პროცედურებითა თუ სახელმძღვანელოებით;

ბ) დაიცვას სამსახურის ინფორმაციის კონფიდენციალობის წესები;

გ) უზრუნველყოს არსებული ინფორმაციული სისტემების, ქსელების, მოწყობილობებისა და კავშირგაბმულობის საშუალებების უსაფრთხო გამოყენება;

დ) დროულად შეატყობინოს შესაბამის უფლებამოსილ პირს აღმოჩენილი ინფორმაციული უსაფრთხოების წესების დარღვევების ან საეჭვო სიტუაციების შესახებ.

7. ინფორმაციული უსაფრთხოების საბჭო

7.1. იუმს-ის დანერგვისა და მუდმივი გაუმჯობესების მიზნით, სამსახურში მოქმედებს ინფორმაციული უსაფრთხოების საბჭო (შემდგომ - საბჭო). საბჭო ეყრდნობა ინფორმაციული უსაფრთხოების პრინციპებს და აღიარებულ სტანდარტებს, შეიმუშავებს/გასცემს რეკომენდაციებს და იღებს სხვა გადაწყვეტილებებს სამსახურის მასშტაბით ინფორმაციულ უსაფრთხოებასთან დაკავშირებულ საკითხებზე, მათ შორის იხილავს ინფორმაციული უსაფრთხოების გეგმას, ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტის პროექტს, ისმენს ინფორმაციული უსაფრთხოების პოლიტიკის გეგმის შესრულების შესახებ პერიოდულ ანგარიშებს, იღებს ინფორმაციას ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციული უსაფრთხოების მენეჯერისაგან.

7.2. საბჭოს შემადგენლობაში შედიან:

ა) სამსახურის უფროსი (საბჭოს თავმჯდომარე);

ბ) სამსახურის უფროსის პირველი მოადგილე;

გ) სამსახურის უფროსის მოადგილე;

დ) ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის უფროსი;

ე) იურიდიული დეპარტამენტის უფროსი;

ვ) ადმინისტრაციული და ეკონომიკური უზრუნველყოფის დეპარტამენტის უფროსი;

ზ) სამსახურის უფროსის აპარატის უფროსი;

თ) შიდა აუდიტი;

ი) ინფორმაციული უსაფრთხოების მენეჯერი;

კ) კომპიუტერული უსაფრთხოების სპეციალისტი;

ლ) შრომის უსაფრთხოების სპეციალისტი.

7.3. საბჭოს მდივნის ფუნქციას ასრულებს სამსახურის უფროსის აპარატის სპეციალისტი/უმცროსი იურისტი

7.4. საბჭოს თავმჯდომარის ინიციატივით ან სამსახურის ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის უფროსის ან ინფორმაციული უსაფრთხოების მენეჯერის რეკომენდაციით, საბჭო იკრიბება არანაკლებ წელიწადში ერთხელ.

7.5. კრიტიკული ინციდენტის შემთხვევაში, საბჭოს თავმჯომარის ინიციატივით ან სამსახურის ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის უფროსის ან ინფორმაციული უსაფრთხოების მენეჯერის რეკომენდაციით, საბჭო იკრიბება დაუყოვნებლივ.

8. პასუხისმგებლობები

8.1. სამსახურის უფროსი, სამსახურის საჭირო რესურსების გამოყოფის, პასუხისმგებლობათა დელეგირებისა და მონაცემთა უსაფრთხოების საკითხების სამართლებრივი რეგულირების გზით, უზრუნველყოფს ინფორმაციული უსაფრთხოების ინიციატივების მხარდაჭერას და იღებს გადაწყვეტილებებს საბჭოს კომპეტენციას მიკუთვნებულ საკითხებზე.

8.2. სამსახურის უფროსის პირველი მოადგილე, მოადგილე და სამსახურის სტრუქტურული ერთეულების ხელმძღვანელები:

ა) კომპეტენციის ფარგლებში, მონაწილეობენ ინფორმაციული უსაფრთხოების შინასამსახურებრივი წესებისა და სამოქმედო გეგმების შემუშავებასა და მათ დანერგვაში;

ბ) პასუხისმგებლები არიან მათ დაქვემდებარებაში არსებული სტრუქტურული ერთეულების/თანამშრომლების მიერ მათი ფუნქციებისა და საქმიანობის ინფორმაციული უსაფრთხოების პოლიტიკის, სტანდარტების, პროცედურების, სახელმძღვანელოების და მასთან დაკავშირებული სხვა დოკუმენტების მოთხოვნების შესაბამისად განხორციელებაზე;

გ) საჭიროების შემთხვევაში, მიმართავენ ინფორმაციული უსაფრთხოების მენეჯერსა და ადმინისტრაციული და ეკონომიკური უზრუნველყოფის დეპარტამენტის უფროსს მათ დაქვემდებარებაში არსებული თანამშრომლებისათვის ინფორმაციული უსაფრთხოების საკითხებზე ზოგადი და დარგობრივი ტრენინგების ჩატარების მოთხოვნით;

დ) ვალდებულნი არიან მათ დაქვემდებარებაში არსებული სტრუქტურული ერთეულების/თანამშრომლების მიერ ინფორმაციული უსაფრთხოების მოთხოვნების გაწზრახ ან გაუფრთხილებლობით დარღვევის ნებისმიერი ფაქტის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდონ სამსახურის უფროსს და ინფორმაციული უსაფრთხოების მენეჯერს;

ე) ასრულებენ სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებულ სხვა ვალდებულებებსა და ღონისძიებებს.

8.3. ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის უფროსი პასუხისმგებელია:

ა) დეპარტამენტის მფლობელობაში არსებულ რესურსებზე პოლიტიკისა და შესაბამისი სტანდარტების გავრცელების უზრუნველყოფაზე;

ბ) ხელი შეუწყოს პოლიტიკიდან და/ან სტანდარტებიდან გამომდინარე კონტროლის მექანიზმების ტესტირებასა და დანერგვას;

გ) უზრუნველყოს დეპარტამენტის მფლობელობაში/მართვაში არსებული ინფორმაციული აქტივებისა და ინფორმაციული სისტემების სათანადო დაცულობა.

დ) ინფორმაციული უსაფრთხოების საბჭოს დავალებით განახორციელოს ინფორმაციული უსაფრთხოების პოლიტიკისა და სამოქმედო გეგმების მოთხოვნების შესრულების მონიტორინგი;

ე) მონაწილეობა მიიღოს ინფორმაციული აქტივებისა და მათზე წვდომის აღწერის ხარისხის უზრუნველყოფის პროცესებში;

ვ) უზრუნველყოს კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზი და ანგარიშგება;

ზ) კომპეტენციის ფარგლებში, მონაწილეობა მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებისა და სამოქმედო გეგმების შემუშავებაში;

თ) შეასრულოს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებული სხვა ვალდებულებები და ღონისძიებები.

8.4. იურიდიული დეპარტამენტის უფროსი:

ა) უზრუნველყოფს პოლიტიკის მოქმედ კანონმდებლობასთან შესაბამისობას;

ბ) უზრუნველყოფს ინფორმაციული უსაფრთხოების შინასამსახურებრივ წესებში და სამოქმედო გეგმებში სამსახურის ორგანიზაციული კონტექსტისა და სპეციფიკის, მათ შორის, პერსონალურ მონაცემთა დაცვის შესახებ კანონის და სხვა საკანონმდებლო აქტების გათვალისწინებას;

გ) უზრუნველყოფს შინასამსახურებრივ წესებში და სამსახურის უფროსის მიერ გამოცემულ ყველა საკანონმდებლო აქტებში ინფორმაციული უსაფრთხოების პოლიტიკით და თანმდევი დოკუმენტებით გათვალისწინებული ვალდებულებების გათვალისწინებას;

დ) გასცემს სამართლებრივ კონსულტაციებს ინფორმაციული უსაფრთხოების ინციდენტების მოკვლევის დროს, ასევე, სხვა სადავო და კონფლიქტურ სიტუაციებში;

ე) ასრულებს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებულ სხვა ვალდებულებებსა და ღონისძიებებს.

8.5. ადმინისტრაციული და ეკონომიკური უზრუნველყოფის დეპარტამენტის უფროსი:

ა) უზრუნველყოფს სამსახურის თანამშრომლებთან, სტაჟიორებთან და მომსახურების ხელშეკრულებებში ინფორმაციულ უსაფრთხოებასთან დაკავშირებული ვალდებულებების გათვალისწინებას;

ბ) უზრუნველყოფს სამსახურის თანამშრომლების, სტაჟიორებისა და მომსახურების ხელშეკრულებით გათვალისწინებული შემსრულებლების ინფორმირებულობას წინამდებარე პოლიტიკის დოკუმენტისა და ინფორმაციული უსაფრთხოების წესების შესახებ;

გ) ინფორმაციული უსაფრთხოების მენეჯერის მიმართვის საფუძველზე, უზრუნველყოფს სამსახურის თანამშრომლებისთვის ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზების მიზნით, აუცილებელი ღონისძიებების განხორციელებას;

დ) ასრულებს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა

და სამოქმედო გეგმებით გათვალისწინებულ სხვა ვალდებულებებსა და ღონისძიებებს.

8.6. სამსახურის უფროსის აპარატის უფროსი უზრუნველყოფს საბჭოს მუშაობის ორგანიზაციულ მხარდაჭერას.

8.7. შიდა აუდიტი ახორციელებს სამსახურის თანამშრომლების მიერ პოლიტიკის შესრულებაზე საერთო მონიტორინგს.

8.8. ინფორმაციული უსაფრთხოების მენეჯერი:

ა) უზრუნველყოფს ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიურ მონიტორინგს;
ბ) აღწერს ინფორმაციულ აქტივებსა და მათზე წვდომის შემთხვევებს;
გ) შეიმუშავებს ინფორმაციული უსაფრთხოების შინაუწყებრივ დოკუმენტაციას ან/და კოორდინაციას უწევს მათ შემუშავებას;
დ) ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ინფორმაციული უსაფრთხოების საბჭოს და სახელმწიფო უსაფრთხოების სამსახურის სფეროში მოქმედ საჯარო სამართლის იურიდიულ პირს – ოპერატიული ტექნიკურ სააგენტოს (შემდგომ – სააგენტო);
ე) კოორდინაციას უწევს ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შესრულებას;
ვ) აგროვებს ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციას და ახორციელებს მათზე რეაგირების მონიტორინგს;
ზ) იღებს გადაწყვეტილებას სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის მიერ ორგანიზაციის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგანზე წვდომის შესაძლებლობის/შეუძლებლობის შესახებ;
თ) კოორდინაციას უწევს ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის ჩატარებას;
ი) უზრუნველყოფს სამსახურის თანამშრომლებისთვის ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზებასა და ჩატარებას;
კ) უზრუნველყოფს ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგებას და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობის წარმართვას;
ლ) ასრულებს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებულ სხვა ვალდებულებებსა და ღონისძიებებს.

8.9. ინფორმაციული უსაფრთხოების მენეჯერი ინფორმაციული უსაფრთხოების საკითხების დამუშავების დროს ანგარიშვალდებულია სამსახურის უფროსისა და ინფორმაციული უსაფრთხოების საბჭოს წინაშე. ყველა მნიშვნელოვანი გადაწყვეტილება, რომლებიც შეეხება პოლიტიკის განხორციელებას, მიიღება აღნიშნული პირების მიერ ან მათთან წინასწარი შეთანხმებით.
8.10. სამსახურში ინფორმაციული უსაფრთხოების მენეჯერის ფუნქციებს ასრულებს ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის უფროსის მოადგილე.

8.11. კომპიუტერული უსაფრთხოების სპეციალისტი:

ა) უზრუნველყოფს კომპიუტერული სისტემების ყოველდღიურ მონიტორინგს და შეფასებას;
ბ) უზრუნველყოფს კომპიუტერული ინციდენტების იდენტიფიცირებას, მათზე რეაგირებას და კომპიუტერული ინციდენტის შესახებ ინფორმაციის დაუყოვნებლივ მიწოდებას ინფორმაციული უსაფრთხოების მენეჯერისთვის და სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფისთვის;
გ) უზრუნველყოფს კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზსა და

ანგარიშგებას;
დ) უზრუნველყოფს სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფთან კოორდინაციას;
ე) კომპეტენციის ფარგლებში მონაწილეობს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებისა და სამოქმედო გეგმების შემუშავებაში;
ვ) ასრულებს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებულ სხვა ვალდებულებებსა და ღონისძიებებს.
8.12.კომპიუტერული უსაფრთხოების სპეციალისტი ინფორმაციული უსაფრთხოების საკითხების დამუშავების დროს ანგარიშვალდებულია სამსახურის უფროსის და ინფორმაციული უსაფრთხოების საბჭოს წინაშე.
8.13. სამსახურში კომპიუტერული უსაფრთხოების სპეციალისტის ფუნქციებს ასრულებს ინფორმაციული ტექნოლოგიებისა და მონიტორინგის დეპარტამენტის ინფორმაციული უსაფრთხოების ადმინისტრატორი.

8.14. შრომის უსაფრთხოების სპეციალისტი პასუხისმგებელია:

ა) ინფორმაციასთან და ინფორმაციულ სისტემებთან დაკავშირებული სივრცეებისა და სამსახურის შენობა-ნაგებობების უსაფრთხოებაზე;
ბ) სამსახურის შენობა-ნაგებობებში, მათ შორის ადმინისტრაციულ შენობაში პერსონალის უსაფრთხოების უზრუნველყოფაზე;
გ) უსაფრთხოების რისკების განსაზღვრაზე, რომლებმაც შეიძლება იმოქმედონ ინფორმაციული უსაფრთხოების სფეროზე;
დ) ინფორმაციის უსაფრთხოებისა და პერსონალის ფიზიკური უსაფრთხოების დარღვევებთან დაკავშირებული ფაქტების გამოვლენასა და მათზე რეაგირებაზე.

8.15. სამსახურის თითოეული თანამშრომელი:

ა) საჭიროების შემთხვევაში, კომპეტენციის ფარგლებში, მონაწილეობს ინფორმაციული უსაფრთხოების შინასამსახურებრივი წესებისა და სამოქმედო გეგმების შემუშავებასა და მათ დანერგვაში;

ბ) ვალდებულია, გაეცნოს ინფორმაციულ უსაფრთხოებასთან დაკავშირებით, წინამდებარე პოლიტიკის დოკუმენტისა და სამსახურის შინასამსახურებრივი წესებით გათვალისწინებულ მოთხოვნებს;

გ) ვალდებულია, დაიცვას სამსახურის ინფორმაციის კონფიდენციალობის წესები;

დ) ვალდებულია, დაიცვას ინფორმაციის დამმუშავებელი მოწყობილობის, ქსელებისა და კავშირგაბმულობის საშუალებების უსაფრთხო გამოყენების წესები;

ე) ვალდებულია, ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევის/სავარაუდო დარღვევის ნებისმიერი ფაქტის შესახებ ინფორმაციის ფლობის ან ასეთი ფაქტის შესახებ ეჭვის არსებობის შემთხვევაში, დაუყოვნებლივ შეატყობინოს თავის უშუალო ხელმძღვანელს, სამსახურის უფროსს და ინფორმაციული უსაფრთხოების მენეჯერს;

ვ) უფლებამოსილია წინამდებარე პოლიტიკის დოკუმენტისა და სამსახურის შინასამსახურებრივი გამოყენების წესებით გათვალისწინებულ საკითხებთან დაკავშირებით ბუნდოვანების შემთხვევაში, კონსულტაციის მიზნით მიმართოს ინფორმაციული უსაფრთხოების მენეჯერს ან/და კომპიუტერული უსაფრთხოების სპეციალისტს;

ზ) უფლებამოსილია თავის უშუალო ხელმძღვანელს მიმართოს ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ჩატარების თხოვნით;

თ) ვალდებულია, შეასრულოს სამსახურის ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესებითა და სამოქმედო გეგმებით გათვალისწინებული სხვა ვალდებულებები და ღონისძიებები.

8.16. მესამე პირები - სამსახურის კონსულტანტები, გარე აუდიტორები, აგრეთვე ყველა სხვა პირი, რომელთათვისაც სამსახურს გადაცემული აქვს წვდომა ფასეულ ინფორმაციაზე ან/და მის დამმუშავებელ მოწყობილობებზე:

ა) ვალდებულნი არიან იმოქმედონ წინამდებარე პოლიტიკის დოკუმენტით განსაზღვრული მოთხოვნების შესაბამისად და ასევე, გაითვალისწინონ აღიარებული ინფორმაციული უსაფრთხოების წესები და სტანდარტები.

ბ) ვალდებულნი არიან წერილობით იკისრონ პასუხისმგებლობა სამსახურის შესაბამისი ინფორმაციის და ინფორმაციული სისტემების დაცვაზე.

8.17. მესამე პირების მიერ სამსახურთან ურთიერთობის დამყარების წინაპირობაა კონფიდენციალობის დაცვისა და გაუვრცელებლობის შეთანხმების (NDA- Non-disclosure agreement) გაფორმება მესამე პირსა და სამსახურს შორის, ან მესამე პირსა და სამსახურს შორის შესაბამის კონტრაქტში/შეთანხმებაში კონფიდენციალობის დაცვისა და გაუვრცელებლობის შეთანხმების მუხლების გათვალისწინება, რომელიც უზრუნველყოფს ფასეულ ინფორმაციაზე ნებადართულ წვდომას.

9. ინფორმაციული აქტივების მართვა

9.1. სამსახურის საკუთრებაში ან მფლობელობაში არსებული ინფორმაციული აქტივები და ინფორმაციული სისტემები განკუთვნილია მხოლოდ სამსახურებრივი მიზნებისათვის. მათი მეშვეობით შექმნილი, მიღებული, შენახული, გადაცემული ან სხვაგვარად დამუშავებული ინფორმაცია ეკუთვნის სამსახურს და არა მის ფაქტობრივ მფლობელს.

9.2. ინფორმაციული აქტივის მფლობელი არის პირი ან სტრუქტურული ერთეული, რომელსაც გააჩნია აქტივის შექმნის, განვითარების, მხარდაჭერის, გამოყენების, დაცვის ან სხვაგვარად დამუშავების დადასტურებული მართვის უფლება.

9.3. ინფორმაციული აქტივების მართვის მიზნით, სამსახურში მოქმედებს:

ა) ინფორმაციული აქტივების მართვის წესი, რომელიც მოიცავს ინფორმაციული აქტივების აღწერის, კლასიფიცირების, ხელმისაწვდომობის, გაცემის (გამოქვეყნების), გამოყენების, შეცვლისა და განადგურების წესებს და სხვა საკითხებს;

ბ) გადაადგილებადი მედია-მატარებლების მართვის პროცედურები;

გ) სხვა წესები და პროცედურები გამოვლენილი საჭიროებების შესაბამისად.

9.4. ინფორმაციული აქტივების მართვის მიზნით, სამსახური:

ა) ატარებს ინფორმაციული სისტემების ინვენტარიზაციას ყველა ინფორმაციული აქტივის გამოვლენისა და აღრიცხვის მიზნით, რომლის შედეგად, ყოველ ინფორმაციულ აქტივს ანიჭებს კრიტიკულობის შესაბამის კლასს;

ბ) ახორციელებს კლასიფიცირებული ინფორმაციის მარკირებას მისი კლასის შესაბამისად;

გ) აღწერს ყოველი ინფორმაციული აქტივის მნიშვნელობას, ფასეულობას, უსაფრთხოებისა და დაცვის არსებულ დონეს;

დ) ინფორმაციული აქტივების აღწერის შემდგომ, აანალიზებს რისკებს მოცემულ აქტივებთან მიმართებით;

ე) ინფორმაციის კლასიფიკაციაზე დაყრდნობით, განსაზღვრავს ინფორმაციული აქტივების დაცვის ხარისხის უზრუნველყოფის ან მოპყრობის წესებს;

ვ) განსაზღვრავს თითოეული ინფორმაციული აქტივის მფლობელს და მის პასუხისმგებლობებს კონტროლის შესაბამის მექანიზმებზე;

ზ) სამსახურის თანამშრომლების ჩართულობით, არა ნაკლებ წელიწადში ერთხელ ახორციელებს ინფორმაციული აქტივების აღწერას, კლასიფიცირებას და უზრუნველყოფს მათ მართვას;
თ) უზრუნველყოფს გადაადგილებადი მედია-მატარებლების მართვას;
ი) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

10. ინფორმაციული უსაფრთხოების ამოცანები

ინფორმაციული უსაფრთხოების 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 შემუშავება, დანერგვა და მხარდაჭერა;

ზ) ინფორმაციული უსაფრთხოების ინციდენტების მართვა;

თ) საქმიანობის უწყვეტობის მართვა;

ი) საკანონმდებლო შესაბამისობა.

11. ადამიანური რესურსების უსაფრთხოება

11.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია სამსახურის თანამშრომლებმა და კონტრაქტორებმა გააცნობიერონ ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მოთხოვნები და პასუხისმგებლობები და შეასრულონ აღნიშნული მოთხოვნები.
11.2. ადამიანური რესურსების უსაფრთხოების მიზნით, სამსახურში მოქმედებს:
ა) სამსახურში დასასაქმებელი კანდიდატების შემოწმების შიდა პროცედურა;
ბ) თანამშრომელთა მიმართ დისციპლინური წარმოების ჩატარების წესი და თანაზომიერი დისციპლინური სახდელები;
გ) სხვა წესები და პროცედურები გამოვლენილი საჭიროებების შესაბამისად.
11.3. ადამიანური რესურსების უსაფრთხოების მიზნით, სამსახური:
ა) სამსახურში დასასაქმებელ ყველა კანდიდატს ამოწმებს საქართველოს კანონმდებლობისა და ეთიკის მოთხოვნათა დაცვით, ამასთან, უზრუნველყოფს, კანდიდატის მიერ განსახორციელებელი საქმიანობის მოთხოვნების, წვდომადი ინფორმაციის კლასიფიკაციისა და წვდომასთან დაკავშირებული რისკების პროპორციულ შემოწმებას;
ბ) დასაქმებულებსა და კონტრაქტორებთან გაფორმებულ ხელშეკრულებებში ითვალისწინებს მხარეთა პასუხისმგებლობებს ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევის შემთხვევაში;
გ) ახორციელებს ინფორმაციული უსაფრთხოების საკითხებზე თანამშრომლებისა და საჭიროების შემთხვევაში, კონტრაქტორების ცნობიერების ამაღლების მიზნით შესაბამის ღონისძიებებს (ტრენინგები/სწავლება და სხვა);

დ) რეგულარულად აწვდის ინფორმაციას თანამშრომლებს სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკებისა და პროცედურების განახლებების შესახებ;

ე) შეისწავლის ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევის შემთხვევებს და თანამშრომლის მიმართ იყენებს თანაზომიერ დისციპლინური პასუხისმგებლობის ზომას, ხოლო სხვა კონტრაქტორისადმი - თანაზომიერ სანქციას;

ვ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

12. ფიზიკური და გარემოს უსაფრთხოება

12.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, სამსახურის თითოეული თანამშრომელი და კონტრაქტორი ვალდებულია, არ დაიშუროს ძალისხმევა ინფორმაციულ აქტივებზე და ინფორმაციის დამმუშავებელ მოწყობილობებზე უნებართვო ფიზიკური წვდომის, დაზიანების ან ჩარევის თავიდან ასარიდებლად.

12.2. ფიზიკური და გარემოს უსაფრთხოების მიზნით, სამსახურში მოქმედებს:

ა) სამსახურის სამუშაო სივრცისა და მოწყობილობების ფიზიკური დაცვის წესები;

ბ) სტიქიური უბედურებებისგან, მავნე პროგრამული შეტევისა ან უბედური შემთხვევისაგან ფიზიკური დაცვის წესები;

გ) სამსახურის დაცულ არეებში მუშაობის პროცედურები;

დ) სხვა წესები და პროცედურები გამოვლენილი საჭიროებების შესაბამისად.

12.3. ფიზიკური და გარემოს უსაფრთხოების მიზნით, სამსახური:

ა) იცავს სამსახურის სამუშაო სივრცეებს, განსაკუთრებით კი იმ ფიზიკურ გარემოს, სადაც განთავსებულია სენსიტიური და კრიტიკული ინფორმაციული აქტივები;

ბ) იცავს სამსახურის ინფორმაციის დამმუშავებელ მოწყობილობებს, დამხმარე და სხვა საშუალებებს უნებართვო წვდომისგან და იმ რისკებისგან, რომლებიც მომდინარეობს გარემოს საფრთხეებისგან;

გ) უზრუნველყოფს სამსახურის ინფორმაციის დამმუშავებელი მოწყობილობების განგრძობად ხელმისაწვდომობასა და მთლიანობას;

დ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

13. კომუნიკაციებისა და ოპერაციების მართვა

13.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია სამსახურში კომუნიკაციებისა (ქსელებში ინფორმაციის და ინფორმაციის დამმუშავებელი მოწყობილობების დაცვა, სამსახურის შიგნით და მის გარეთ ინფორმაციის გადაცემის უსაფრთხოების უზრუნველყოფა და სხვა) და ოპერაციების (ინფორმაციის დამმუშავებელი მოწყობილობების გამართული და უსაფრთხო ფუნქციონირების უზრუნველყოფა, ოპერაციული სისტემების მთლიანობის უზრუნველყოფა, ტექნიკური სისუსტეების პრევენცია და სხვა) მართვა და მათი უსაფრთხოება.

13.2. კომუნიკაციების მართვისა და უსაფრთხოების მიზნით, სამსახურში:

ა) მოქმედებს ინფორმაციის გადაცემის წესები და პროცედურები;

ბ) შემუშავებულია შეთანხმებები ინფორმაციის კონფიდენციალობის ან გაუმჟღავნებლობის შესახებ;

გ) შემუშავებულია სხვა წესები და პროცედურები გამოვლენილი საჭიროებების შესაბამისად.

13.3. კომუნიკაციების მართვისა და უსაფრთხოების მიზნით, სამსახური:

ა) უზრუნველყოფს ქსელების მართვასა და კონტროლს, რათა დაცულ იქნეს ინფორმაცია სისტემებსა და პროგრამულ უზრუნველყოფებში;

ბ) უზრუნველყოფს ქსელური მომსახურებების უსაფრთხოებას და ქსელების გამიჯვნას;

გ) ახორციელებს ინფორმაციის უსაფრთხო გადაცემისთვის აუცილებელ ღონისძიებებს;

დ) ახორციელებს ელექტრონული მიმოწერის უსაფრთხოებისთვის აუცილებელ ღონისძიებებს;

ე) საჭიროების შემთხვევაში, საქმიანი ინფორმაციის უსაფრთხო გადაცემასთან დაკავშირებით, სამსახურსა და მესამე პირებს შორის დებს შეთანხმებას;

ვ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

13.4. ოპერაციების მართვისა და უსაფრთხოების მიზნით, სამსახური:

ა) ახორციელებს საოპერაციო პროცედურების დოკუმენტირებას, რათა უზრუნველყოფილ იქნეს ინფორმაციის დამმუშავებელი მოწყობილობების გამართული და უსაფრთხო ფუნქციონირება;

ბ) იცავს ინფორმაციისა და ინფორმაციის დამმუშავებელ მოწყობილობებს მავნე პროგრამული კოდისგან;

გ) აწარმოებს ინფორმაციის სარეზერვო ასლებს;

დ) ახორციელებს მოვლენების ლოგირებასა და მონიტორინგს;

ე) უზრუნველყოფს ოპერაციული სისტემების კონტროლსა და ტექნიკური სისუსტეების მართვას;

ვ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

14. ინფორმაციულ აქტივებზე წვდომის კონტროლი

14.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია სამსახურში ინფორმაციულ აქტივებზე წვდომის კონტროლის დანერგვა.

14.2. ინფორმაციულ აქტივებზე წვდომის კონტროლის მიზნით, სამსახური:

ა) უზრუნველყოფს მომხმარებელთა წვდომის მართვას;

ბ) აკონტროლებს სისტემასა და პროგრამულ უზრუნველყოფაზე წვდომას;

გ) ინფორმაციის კონფიდენციალობის, ავთენტურობის ან/და მთლიანობის დაცვის მიზნით, იყენებს კრიპტოგრაფიას;

დ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

14.3. „ინფორმაციულ აქტივებზე წვდომის კონტროლთან დაკავშირებული საკითხები განისაზღვრება სამსახურის ინფორმაციულ აქტივებზე წვდომის კონტროლის დოკუმენტით.

15. ინფორმაციული სისტემების შეძენა, შემუშავება და მხარდაჭერა

15.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, სამსახური ითვალისწინებს ინფორმაციული უსაფრთხოების მოთხოვნებსა და სტანდარტებს ინფორმაციული სისტემის მთელი სასიცოცხლო ციკლის მანძილზე.

15.2. სამსახური უზრუნველყოფს უსაფრთხოების შესაბამისი ღონისძიებების განხორციელებას ინფორმაციული სისტემების შეძენის, შემუშავებისა და მხარდაჭერის პროცესში.

16. ინფორმაციული უსაფრთხოების ინციდენტების მართვა

16.1. ინფორმაციული უსაფრთხოების მიზნით, მნიშვნელოვანია ინფორმაციული უსაფრთხოების ინციდენტების დროული გამოვლენა და მათი შემდგომი სწრაფი, ეფექტური და თანმიმდევრული მართვა.

16.2. სამსახურის თითოეული თანამშრომელი და მესამე პირები ვალდებულნი არიან აცნობონ სამსახურს აღმოჩენილი უსაფრთხოების სისუსტის ან ასეთი სავარაუდო ფაქტის შესახებ.

16.3. ინფორმაციული უსაფრთხოების ინციდენტების მართვის მიზნით, სამსახურში მოქმედებს ინციდენტების მართვის პროცედურა და საჭიროების შემთხვევაში სხვა შესაბამისი პროცედურები, რომლებიც განისაზღვრება ინფორმაციული უსაფრთხოების ინციდენტების მართვის პოლიტიკის დოკუმენტით.

16.4. ინფორმაციული უსაფრთხოების ინციდენტების მართვის მიზნით, სამსახური:

ა) უზრუნველყოფს ინფორმაციული უსაფრთხოების მოვლენებისა და სისუსტეების შესახებ ანგარიშგებას;

ბ) უზრუნველყოფს ინფორმაციული უსაფრთხოების ინციდენტებზე სწრაფ და ეფექტურ რეაგირებას;

გ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

17. საქმიანობის უწყვეტობის მართვა

17.1. ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია ინფორმაციული უსაფრთხოების უწყვეტობა ინტეგრირებულ იქნეს სამსახურის საქმიანობის უწყვეტობის მართვის სისტემებში.

17.2. საქმიანობის უწყვეტობის მართვის მიზნით, სამსახურში მოქმედებს:

ა) ინფორმაციული უსაფრთხოების უწყვეტობისადმი არასასურველ სიტუაციებში (მაგალითად, კრიზისის ან კატასტროფის დროს) მოქმედების პროცედურები და ინფორმაციული უსაფრთხოების უწყვეტობის კონტროლის მექანიზმები;

ბ) სხვა წესები და პროცედურები გამოვლენილი საჭიროებების შესაბამისად.

17.3. საქმიანობის უწყვეტობის მართვის მიზნით, სამსახური:

ა) ნერგავს პროცედურებსა და კონტროლის მექანიზმებს, რომლებიც უზრუნველყოფენ ინფორმაციული უსაფრთხოების უწყვეტობას არასასურველ სიტუაციებში;

ბ) პერიოდულად ამოწმებს უკვე ჩამოყალიბებულ და დანერგილ ინფორმაციული უსაფრთხოების უწყვეტობის კონტროლის მექანიზმებს, რათა უზრუნველყოს მათი ქმედითობა და ეფექტიანობა არასასურველ სიტუაციებში;

გ) ახორციელებს სხვა ღონისძიებებს გამოვლენილი საჭიროებების შესაბამისად.

18. კანონმდებლობის მოთხოვნებთან შესაბამისობა

18.1. ინფორმაციული უსაფრთხოების მიზნით, მნიშვნელოვანია საკანონმდებლო შესაბამისობის უზრუნველყოფა, რომელიც გულისხმობს:

ა) სამსახურის საქმიანობის მარეგულირებელ სამართლებრივ ნორმებთან შესაბამისობას;

ბ) მესამე პირებთან დადებულ სახელშეკრულებო ურთიერთობებთან შესაბამისობას;

გ) ინფორმაციული უსაფრთხოებისა და პერსონალურ მონაცემთა დაცვის კანონმდებლობასა და სტანდარტებთან შესაბამისობას.

18.2. საკანონმდებლო შესაბამისობის უზრუნველყოფის მიზნით, სამსახური:

ა) დაგეგმილი პერიოდულობით განახორციელებს შიდა აუდიტს იუმს-ის თაობაზე შემდეგი ინფორმაციის მისაღებად: იუმს-ის სამსახურის მიერ განსაზღვრულ მოთხოვნებთან შესაბამისობა; იუმს-ის ინფორმაციული უსაფრთხოების სფეროში არსებული ნორმატიული აქტების მოთხოვნებთან შესაბამისობა; იუმს-ის ეფექტიანად დანერგვა და მისი მხარდაჭერა.

ბ) დაგეგმავს, ჩამოაყალიბებს, დანერგავს და მართავს აუდიტის პროგრამას/პროგრამებს;

გ) საჭიროების შემთხვევაში, გამოიყენებს შესაბამისობის შემოწმების სხვა მექანიზმებს;

დ) უზრუნველყოფს გამოვლენილ საჭიროებებზე რეაგირებას.

19. პოლიტიკის შესრულება

19.1. წინამდებარე პოლიტიკის დებულებების ნებისმიერი სახით დაუცველობა ან დარღვევა, რომელმაც სამსახურს შესაძლოა, მიაყენოს მატერიალური ან არამატერიალური ზიანი, გამოიწვევს შესაბამისი სამართლებრივი ან ადმინისტრაციული ზომების გამოყენებას დამრღვევის მიმართ, რაც დამოკიდებულია დარღვევის სერიოზულობის ხარისხსა და მის შედეგად დამდგარ ზიანზე.

19.2. ინფორმაციის და ინფორმაციული სისტემების ყველა აღმოჩენილი უნებართვო გამოყენება და სხვა სახის შეუსაბამობა ან ინციდენტი გამოკვლეული იქნება სამსახურში არსებული პროცედურების შესაბამისად, რაზეც ზედამხედველობას ახორციელებს ინფორმაციული უსაფრთხოების მენეჯერი.

20. პოლიტიკის გადახედვა

20.1. იუმს-ის ეფექტიანობის და კანონმდებლობასთან შესაბამისობის უზრუნველყოფის მიზნით, პოლიტიკა ექვემდებარება პერიოდულ განხილვას/გადახედვას საბჭოს მიერ და საჭიროების შემთხვევაში, ცვლილებების ინიცირებას.

20.2. პოლიტიკის გადახედვის საფუძველი შეიძლება ასევე გახდეს:

ა) სამსახურში განხორციელებული მნიშვნელოვანი ორგანიზაციული/ტექნიკური ცვლილებები;

ბ) ინფორმაციული უსაფრთხოების სფეროში არსებული ნორმატიული აქტების მოთხოვნების ცვლილებები;

გ) შიდა აუდიტის/გარე აუდიტის შედეგები;

დ) სხვა გარემოებები, მიმართული ინფორმაციული უსაფრთხოების სისტემის გაუმჯობესებისაკენ.

21. გამონაკლისები

თუ ვერ სრულდება პოლიტიკით, სტანდარტებით, პროცედურებით, სახელმძღვანელოებითა და მათთან დაკავშირებული სხვა დოკუმენტებით გათვალისწინებული შესაბამისი უსაფრთხოების კონტროლის მექანიზმების ზოგიერთი მოთხოვნა, ინფორმაციული უსაფრთხოების მენეჯერი აღნიშნულს წერილობით აცნობებს საბჭოს, რომლის თანხმობის შემთხვევაშიც, შესაძლოა, მოხდეს შესაბამისი გამონაკლისის დაშვება.