საქართველოს ფინანსთა სამინისტრო

სსიპ საფინანსო-ანალიტიკური სამსახური

ბრძანება N 43

18/03/2019 ქ.თბილისი

საჯარო სამართლის იურიდიული პირის - საფინანსო ანალიტიკური სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების მართვის სისტემების გავრცელების სფეროს დამტკიცების შესახებ

საქართველოს ფინანსთა მინისტრის 2010 წლის 31 მარტის №247 ბრძანებით დამტკიცებული „საჯარო სამართლის იურიდიული პირის - საფინანსო-ანალიტიკური სამსახურის დებულების“ მე-3 მუხლის მე-3 პუნქტის „გ“ ქვეპუნქტის საფუძველზე,

ვ ბ რ ძ ა ნ ე ბ:

1. დამტკიცდეს საჯარო სამართლის იურიდიული პირის - საფინანსო-ანალიტიკური სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკა წინამდებარე ბრძანებაზე თანდართული დანართი N1-ის შესაბამისად.
2. დამტკიცდეს საჯარო სამართლის იურიდიული პირის - საფინანსო-ანალიტიკური სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემების გავრცელების სფერო წინამდებარე ბრძანებაზე თანდართული დანართი N2-ის შესაბამისად.
3. დაევალოს საჯარო სამართლის იურიდიული პირის - საფინანსო-ანალიტიკური სამსახურის ადმინისტრაციულ დეპარტამენტს წინამდებარე ბრძანების სხვა დაინტერესებული პირებისათვის კანონმდებლობით განსაზღვრული წესით გაცნობა.
4. ბრძანება შეიძლება გასაჩივრდეს მისი გაცნობიდან ერთი თვის ვადაში ქ. თბილისის საქალაქო სასამართლოში (მის: ქ. თბილისი, დავით აღმაშენებლის ხეივანი მე-12 კმ, №6) კანონმდებლობით დადგენილი წესით.

ჯონი შურღულაია

სამსახურის უფროსის მოვალეობის შემსრულებელი

დანართი N1

ინფორმაციული უსაფრთხოების პოლიტიკა

ტელ: +995 32 226 15 64

მისამართი: გორგასლის ქუჩა 16, თბილისი 0114, საქართველო

თავი I

ზოგადი დებულებები

მუხლი 1. შესავალი

1. წინამდებარე დოკუმენტი განსაზღვრავს სსიპ საფინანსო-ანალიტიკური სამსახურის (შემდგომში - სამსახური) ინფორმაციული უსაფრთხოების პოლიტიკას, პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და განვითარების მექანიზმებს სამსახურის სამუშაო პროცეს(ებ)ში.

2. წინამდებარე წესის შესაბამისი კომპონენტების დაცვა სავალდებულოა ყველა იმ შიდა თუ გარე პირისთვის, რომლებიც თავიანთ საქმიანობაში იყენებენ სამსახურის ინფორმაციულ ტექნოლოგიებს, ინფორმაციულ აქტივებსა და რესურსებს.

3. სამსახურის საინფორმაციო ტექნოლოგიების მომხმარებელი ვალდებულია ამ წესის გარდა დაიცვას საქართველოს კანონმდებლობით დადგენილი მოთხოვნები მათ შორის: ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის (მონაცემების) დაცვასთან დაკავშირებით.

4. სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკა ეფუძნება ინფორმაციული უსაფრთხოების საერთაშორისოდ მიღებული სტანდარტების **ISO 27000** ჯგუფს.

5. ინფორმაციული უსაფრთხოების პოლიტიკა, უზრუნველყოფს სამსახურის მიერ კანონმდებლობით განსაზღვრული ფუნქციებისა და უფლებამოსილებების განხორციელებისას ამ პოლიტიკით გათვალისწინებული დებულებების დაცვას.

6. ინფორმაციული უსაფრთხოების პოლიტიკა განსაზღვრავს სამსახურის თანამშრომელთა და სხვა მომხმარებელთა მიერ ინფორმაციის, ინფორმაციული აქტივების, ინფორმაციული ტექნოლოგიებისა და სისტემების მოხმარების წესს.

მუხლი 2. ორგანიზაციული კონტექსტი

ორგანიზაციის მისია: სამსახურის მისიაა, საქართველოს ფინანსთა სამინისტროს (შემდგომში - „სამინისტრო“) და სხვა სახელმწიფო უწყებების ბიზნეს-პროცესების ავტომატიზაცია. ავტომატიზებული ელექტრონული სისტემების ბიზნეს-უწყვეტობისა და ინფორმაციული უსაფრთხოების უზრუნველყოფა. ელექტრონული მმართველობის ხელშეწყობა.

ორგანიზაციის მიზნები:

1. სამინისტროს ეფექტიანი ფუნქციონირებისა და განვითარებისათვის საჭირო საინფორმაციო-საკომუნიკაციო ინფრასტრუქტურის შექმნა, მომსახურება, მისი საიმედო და ეფექტური მუშაობის და განვითარების უზრუნველყოფა;
2. სამინისტროს უწყვეტად ფუნქციონირების ხელშეწყობა და მისი ინფორმაციული უსაფრთხოების უზრუნველყოფა;
3. თავისი კომპეტენციის ფარგლებში სამინისტროს ინფორმაციული და ანალიტიკური მხარდაჭერა;
4. სამინისტროს საინფორმაციო სისტემების ქვეყნის საინფორმაციო-საკომუნიკაციო სივრცეში ინტეგრაცია;
5. საინფორმაციო სისტემების და ახალი სერვისების დანერგვა და განვითარება;
6. მაღალი სტანდარტებისა და ხარისხის ელექტრონული მმართველობის კომპონენტების შექმნა, დანერგვა, შესაბამისი მომსახურება და გაუმჯობესება;
7. სახელმწიფო სექტორის ბიზნეს-პროცესების შესწავლა, ფორმალიზება, ოპტიმიზაცია და ავტომატიზაცია;
8. ქვეყანაში ელექტრონული მთავრობისა და ელექტრონული მმართველობის პოლიტიკის შემუშავებისა და დამკვიდრების ხელშეწყობა;

9. სპეციალიზებული პროგრამული უზრუნველყოფის შექმნა, დანერგვა, განვითარება, ადმინისტრირება და მომსახურება.

აღნიშნული მიზნების მიღწევა საჭიროებს სამუშაო პროცესებში მიღებული ინფორმაციის, სანდო და ეფექტური საშუალებებით დამუშავებას, რაც გულისხმობს თანამედროვე, დახვეწილი და უსაფრთხო ინფორმაციული ტექნოლოგიების გამოყენებას; რაც თავისთავად ხელს შეუწყობს, ორგანიზაციის მიერ საკუთარი უფლებამოსილების განხორციელებისას დამუშავებული ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის ხარისხის ამაღლებას.

ორგანიზაციის ხედვა: სამსახურის ხედვაა, გახდეს ყველაზე წარმატებული სახელმწიფო უწყება რეგიონში საინფორმაციო-საკომუნიკაციო ტექნოლოგიების სფეროში.

სამსახურის საქმიანობის მნიშვნელობა: იმის გათვალისწინებით, რომ სამსახური არის კრიტიკული ინფორმაციული სისტემის სუბიექტი, შესაბამისად მისი ინფორმაციული სისტემ(ებ)ის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის. სამსახურის საქმიანობა დაკავშირებულია ინფორმაციის დამუშავება-შენახვასთან. შესაბამისად სამუშაო პროცესებში ხდება სხვადასხვა სახის ინფორმაციული აქტივების დამუშავება (შექმნა, გამოყენება, გადაცემა და განადგურება). სწორედ ამ უკანასკნელის გათვალისწინებით კრიტიკულად მნიშვნელოვანია აღნიშნული ინფორმაციის სათანადო დონეზე დაცვა.

ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანია: ხელი შეუწყოს სამსახურს ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის სათანადო ხარისხის უზრუნველყოფაში, ინფორმაციული უსაფრთხოების პოლიტიკის გავრცელების სფეროში ისეთი პროცესების ჩამოყალიბებაში, რაც ერთის მხრივ გამოავლენს ინფორმაციული უსაფრთხოების კუთხით არსებულ ხარვეზებს, ხოლო მეორე მხრივ გააუმჯობესებს ინფორმაციული აქტივების დამუშავებისათვის განკუთვნილი პროცესების დაგეგმარების, შესრულებისა და შემოწმების პროცესს.

მოლოდინები: ინფორმაციული უსაფრთხოების მართვის სისტემა ხელს შეუწყობს სამსახურის მიერ დამუშავებული ინფორმაციის სანდოობის ხარისხის ამაღლებას, გაზრდის სამსახურის რეპუტაციას, პროდუქტიულობას, კლიენტების რაოდენობას და მათ კმაყოფილებას, პროცესების ეფექტიანი მუშაობის ხარისხს; შეამცირებს ბიზნეს რისკებს და მნიშვნელოვნად გაიზრდება თანამშრომელთა ფიზიკური უსაფრთხოების ხარისხის დონე.

მუხლი 3. ტერმინთა განმარტებები

დოკუმენტში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) ინფორმაციული აქტივი (შემდგომში - „აქტივი“) - ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სამსახურისთვის, ამასთან ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

ბ) კონფიდენციალურობა - ინფორმაციის მახასიათებელი, რომელიც გულისხმობს მხოლოდ ავტორიზებული სუბიექტებისთვის ან პროცესებისთვის მოთხოვნის შესაბამისად ინფორმაციის ხელმისაწვდომობას;

გ) მთლიანობა - აქტივის სიზუსტისა და სისრულის მახასიათებელი, უტყუარი ცოდნა იმისა, რომ ძირითადი მონაცემები და ინფორმაცია არის სწორი, არ არის შეცვლილი არა-ავტორიზებული პირების მიერ და ასახავს ზუსტ ფაქტებს;

დ) ხელმისაწვდომობა - ავტორიზებული სუბიექტის მიერ მოთხოვნის შესაბამისად, წვდომისა და გამოყენებადობის მახასიათებელი, ანუ უტყუარი ცოდნა იმისა, რომ ინფორმაცია საჭირო დროს იქნება ხელმისაწვდომი ავტორიზებული მომხმარებლებისთვის;

ე) ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) - მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნეს რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა. მხარდაჭერა და მუდმივი გაუმჯობესება;

ვ) ინფორმაციული უსაფრთხოება - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენთიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას. აღნიშნული საქმიანობა უზრუნველყოფს ინფორმაციისა და ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის შენარჩუნებას და დაცვას;

ზ) ინფორმაციული უსაფრთხოების პოლიტიკა (შემდგომში - ,,პოლიტიკა“) - სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემის, საქართველოს კანონით ინფორმაციული უსაფრთხოების შესახებ, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმების, ინსტრუქციების, პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს;

თ) ინფორმაციული აქტივი (შემდგომში - „აქტივი“) - ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სამსახურისთვის, ამასთან ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

ი) კონტროლის მექანიზმი - ინფორმაციული უსაფრთხოების მართვის სახელმძღვანელო პრინციპები, მიმართული საფრთხესთან დაკავშირებული ალბათობის ან/და უარყოფითი შედეგების შესამცირებლად. კერძოდ, ოპერაციების განხორციელებაზე შეზღუდვებისა და წესების შესრულების უზრუნველსაყოფად შექმნილი ქმედებების და ტექნოლოგიების ერთობლიობა;

კ) კრიტიკული ინფორმაციული სისტემის სუბიექტი - სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის;

ლ) ავტორიზებული მომხმარებელი – პირი, რომელსაც შესაბამისი უფლებამოსილი პირისგან გააჩნია თანხმობა ისარგებლოს ინფორმაციით, ინფორმაციული სისტემებით, ინფორმაციული ტექნოლოგიებით და ახორციელებდეს მათ მართვას;

მ) მფლობელი – პირი ან ორგანიზაციული ერთეული, რომელსაც გააჩნია აქტივის შემუშავების, განვითარების, მხარდაჭერის, გამოყენების და დაცვის დადასტურებული მართვის უფლება. „მფლობელი“ არ ნიშნავს, რომ მას გააჩნია აქტივზე რაიმე სახის საკუთრების უფლება;

ნ) თანამშრომელი - სამსახურში შტატით გათვალისწინებულ თანამდებობაზე დასაქმებული ან/და შრომითი ხელშეკრულებით დასაქმებული პირები, რომელიც ვალდებულია განახორციელოს მასზე დაკისრებული ფუნქცია-მოვალეობები.

მუხლი 4. ინფორმაციული უსაფრთხოების საკანონმდებლო ბაზა, პოლიტიკის მიზანი და რეგულირების სფერო

ა) ვინაიდან „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 29 აპრილის N312 დადგენილების თანახმად, სსიპ საფინანსო ანალიტიკური სამსახური წარმოადგენს კრიტიკული ინფორმაციული სისტემის სუბიექტს, სამსახური იღებს ვალდებულებას მიიღოს ინფორმაციული უსაფრთხოების შინა-სამსახურებრივი გამოყენების წესები, რომლებიც ემსახურება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას;

ბ) სსიპ საფინანსო ანალიტიკური სამსახური მოწოდებულია მონაცემთა გაცვლის სააგენტოს თავმჯდომარის, 2013 წლის 4 თებერვლის №2 ბრძანების „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ შესაბამისად, განახორციელოს ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში „იუმს“) ჩამოყალიბება, დანერგვა, ფუნქციონირება, ზედამხედველობა, მხარდაჭერა და გაუმჯობესება საკანონმდებლო რეგულირების ფარგლებში;

გ) ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს სამსახურში ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას;

დ) პოლიტიკა წარმოადგენს საწყის ბაზისს, რომლის საფუძველზეც, დამატებით ინფორმაციული უსაფრთხოების მენეჯერის წარდგინებით, სამსახურის უფროსის მიერ დამტკიცდება ინფორმაციული უსაფრთხოების დეტალური სტანდარტები, პროცედურები, სახელმძღვანელოები;

ე) პოლიტიკის საფუძველზე მიღებული დამატებითი სტანდარტები, თემატიკიდან გამომდინარე, საჭიროებისამებრ გავრცელდება სამსახურზე, კონკრეტულ სუბიექტებზე ან კონკრეტულ თანამდებობებზე;

ვ) ინფორმაციული უსაფრთხოების პოლიტიკის მიზანია სამსახურში არსებული ინფორმაციის, კანონმდებლობით დაკისრებული ფუნქციებისა და რეპუტაციის დასაცავად კონტროლის მექანიზმების შექმნა და მისი მეშვეობით კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფა;

ზ) პოლიტიკა მიზნად ისახავს შიდა და გარე საფრთხეების მიმართ ინფორმაციული უსაფრთხოების დამცავი მექანიზმების, კრიზისული სიტუაციებისა და განზრახ დაზიანების წინააღმდეგ ქცევის ძირითადი წესების შექმნას;

თ) სამსახური გამოხატავს ურყევ ნებას დანერგოს ინფორმაციული უსაფრთხოების მართვის სისტემა, რათა შექმნას ინფორმაციული უსაფრთხოების შესაბამისი კონტროლის მექანიზმები, საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობის მისაღწევად, რაც ხელს შეუწყობს, პოლიტიკის გავრცელების სფეროში არსებული პროცესების უწყვეტობას და ინფორმაციის სათანადო დაცვას.

მუხლი 5. სსიპ საფინანსო ანალიტიკური სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

აღნიშნულის გათვალისწინებით, ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო განსაზღვრულია დანართი 1-ის შესაბამისად.

მუხლი 6. ინფორმაციული უსაფრთხოების პოლიტიკის ამოცანები:

1. ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს სამსახურში ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების შექმნას;
2. ინფორმაციული უსაფრთხოების პოლიტიკის დაცვის სფეროს წარმოადგენს:
   ა) სამსახურის ინფორმაციული ტექნოლოგიების და სისტემების ინფრასტრუქტურა;
   ბ) სამსახურში არსებული ძირითადი მონაცემები და ინფორმაცია;

გ) პირები, რომლებიც იყენებენ ინფორმაციულ სისტემებს ან/და ახორციელებენ მის ადმინისტრირებას;

დ) პირები, რომლებიც ახორციელებენ ძირითადი მონაცემებისა და ინფორმაციის მართვას.

3. პოლიტიკა განსაზღვრავს:

ა) სამსახურის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;

ბ) პასუხისმგებლობებს და როლებს ინფორმაციულ უსაფრთხოებაზე.

მუხლი 7. ინფორმაციული უსაფრთხოების პოლიტიკის სუბიექტები

1) პოლიტიკის რეგულირების სფერო ვრცელდება სამსახურის შემდეგ თანამშრომლებსა და სხვა მომხმარებლებზე.

ა) სამსახურის თანამშრომლებზე;

ბ) ხელშეკრულების საფუძველზე დასაქმებულ პირებზე;

გ) პირზე, რომელიც სამსახურის სიტემაში გადის სტაჟირებას;

დ) პირზე, რომელსაც შეიძლება მიეცეს დაშვება სამსახურის ძირითად მონაცემებთან ან ინფორმაციასთან.

2) სუბიექტები ვალდებულნი არიან დაიცვან პოლიტიკის მოთხოვნები და აიღონ პასუხისმგებლობა მათთვის დაწესებული სტანდარტებისა და წესების სრულყოფილად და ზედმიწევნით შესრულებაზე.

მუხლი 8. ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი მიმართულებები

1) სამსახურის ორგანიზაციული სპეციფიკიდან გამომდინარე, წარმოადგენს რა კრიტიკული ინფორმაციული სისტემის მქონე სუბიექტს, რომლის ინფორმაციული სისტემის გამართული და უწყვეტი ფუნქციონირება მნიშვნელოვანია ორგანიზაციის მიზნების და ამოცანების დაუბრკოლებლად განხორციელებისათვის, ამ დოკუმენტის და სხვა გამომდინარე დოკუმენტების მეშვეობით, უზრუნველყოფს ტექნიკური საშუალებების გამართულად ფუნქციონირებას და ინფორმაციული აქტივების კონფიდენციალურობას, მთლიანობას და ხელმისაწვდომობას. აღნიშნული მიზნის მისაღწევად გამოიყოფა შემდეგი მიმართულებები:

სამსახურის ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი მიმართულებებია:

ა) ინფორმაციული უსაფრთხოების მართვის სისტემის შექმნა - მოიცავს:

ა.ა) ინფორმაციული უსაფრთხოების მართვის სისტემის შექმნას;

ა.ბ) ინფორმაციული უსაფრთხოების ქმედებათა კოორდინირებას, მონიტორინგისა და აუდიტის სისტემის აწყობას;

ა.გ) პასუხისმგებლობათა გადანაწილებას ინფორმაციული აქტივების მფლობელ პირებზე, გარე უსაფრთხოებას - მესამე პირებთან, კონტრაქტორებთან, მომხმარებლებთან ურთიერთობა და ა.შ.

ბ) ინფორმაციული აქტივების მართვა - მოიცავს:

ბ.ა) ინფორმაციული აქტივების აღწერას;

ბ.ბ) აქტივების მფლობელების იდენტიფიცირებას და აქტივების კლასიფიკაციას;

ბ.გ) ორგანიზაციული ჩანაწერებისა და მონაცემების დაცვას;

ბ.დ) პერსონალური მონაცემების შემცველი ინფორმაციის დაცვას და ხელშეუხებლობას;

ბ.ე) ყველა სახის ინფორმაციის და ცოდნის (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის

დამუშავების შესახებ) დაცვას, რომელიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის.

გ) ინფორმაციული უსაფრთხოების რისკების მართვა - მოიცავს:

გ.ა) რისკების იდენტიფიცირებას (სისუსტეებისა და საფრთხეების გამოვლენა);

გ.ბ) გავლენის შეფასებას და რისკის დადგომის ალბათობის განსაზღვრას და რისკის მოპყრობას;

გ.გ) კონტროლის მექანიზმების შემუშავებას.

დ) ადამიანური რესურსების უსაფრთხოება - მოიცავს:

დ.ა) სამსახურში მიღებას და სამუშაო პირობებს;

დ.ბ) სამსახურეობრივი ფუნქცია-მოვალეობების განხორციელების დაწყებას/შეწყვეტას;

დ.გ) აქტივების მიღება/დაბრუნებას და სხვა საკითხებს, რომლებიც დაკავშირებულია შრომით ურთიერთობებთან;

დ.დ) სწავლების, ტრენინგებისა და ინსტრუქტაჟის მეთოდებს თანამშრომელთა უსაფრთხოების უზრუნველსაყოფად;

დ.ე) კონტრაქტორებთან, დაინტერესებულ მხარეებთან ურთიერთობას და ა.შ.

ე) ფიზიკური უსაფრთხოება და გარემო პირობების უსაფრთხოება - მოიცავს:

ე.ა) ფიზიკური უსაფრთხოების პარამეტრებს;

ე.ბ) ოფისების, ოთახების და ძირითადი საშუალებების უსაფრთხოებას;

ე.გ) ინფორმაციულ აქტივებზე ფიზიკური წვდომის კონტროლს, აპარატურის უსაფრთხოებას, ქსელის უსაფრთხოებას, აპარატურის მხარდაჭერას, მისი ხმარებიდან ამოღებისა და უტილიზაციის წესებს.

ვ) ინფორმაციული უსაფრთხოების ინციდენტების მართვა - მოიცავს:

ვ.ა) ინფორმაციული უსაფრთხოების შემთხვევებისა და სისუსტეების შესახებ ანგარიშგებას;

ვ.ბ) ინციდენტების აღწერას, შესწავლას და მათზე ადეკვატურ რეაგირებას;

ვ.გ) ინფორმაციული უსაფრთხოების ინციდენტებისა და გაუმჯობესებების მართვას.

ზ) კომუნიკაციებისა და ოპერაციების მართვა - მოიცავს:

ზ.ა) საოპერაციო პროცედურებს და პასუხისმგებლობების გადანაწილებას;

ზ.ბ) მესამე მხარის მიერ შემოთავაზებული სერვისების მართვას;

ზ.გ) სისტემის დაგეგმვას და მართვას;

ზ.დ) მავნე მობილური კოდებისგან დაცვას; სარეზერვო ასლების შექმნას, ქსელის უსაფრთხოების მართვას;

ზ.ე) ინფორმაციის მედია-მატარებლების მართვას და მონიტორინგს;

ზ.ვ) საარქივო მასალების უსაფრთხოდ შენახვას და მართვას.

თ) წვდომის კონტროლის მართვა - მოიცავს:

თ.ა) მომხმარებელთა წვდომის მართვას და შესაბამის პასუხისმგებლობებს;

თ.ბ) ქსელურ რესურსებზე წვდომის კონტროლს;

თ.გ) ოპერაციულ სისტემებზე წვდომის კონტროლს;

თ.დ) პროგრამებისა და ინფორმაციაზე წვდომის კონტროლს, მობილურ ტექნოლოგიებს და დისტანციურ მუშაობას.

ი) ინფორმაციული სისტემების შეძენა, დანერგვა და მხარდაჭერა - მოიცავს:

ი.ა) ინფორმაციული სისტემების უსაფრთხოების მოთხოვნების შემუშავებას;

ი.ბ) კრიპტოგრაფიული კონტროლის მექანიზმების გამოყენებას;

ი.გ) სისტემური ფაილების უსაფრთხოებას, შემუშავებისა და მხარდაჭერის პროცესების უსაფრთხოებას და ტექნიკური სისუსტეების მართვას.

კ) ბიზნეს-უწყვეტობის მართვა - მოიცავს:

კ.ა) ინფორმაციული უსაფრთხოების ჩართვას ბიზნეს უწყვეტობის პროცესში;

კ.ბ) უწყვეტობის გეგმის შემუშავებას და განხორციელებას;

კ.გ) უწყვეტობის გეგმის შემუშავებას, განხორციელებას, გეგმის ტესტირებას, მხარდაჭერას და ხელახალ შეფასებას.

ლ) შესაბამისობა - მოიცავს:

ლ.ა) პოლიტიკის მუდმივ კონტროლს მოქმედ კანონმდებლობასთან თავსებადობის უზრუნველყოფის მიზნით;

ლ.ბ) საერთაშორისოდ აღიარებულ სტანდარტებთან შესაბამისობას.

2. ინფორმაციული უსაფრთხოების პოლიტიკით განსაზღვრულ მიმართულებებთან დაკავშირებით გადაწყვეტილება მიიღება, რისკების მართვის მეთოდოლოგიის შესაბამისად.

3. ინფორმაციული უსაფრთხოების რისკების მართვა ხორციელდება, ინფორმაციული უსაფრთხოების რისკების მართვის მეთოდოლოგიის შესაბამისად მიღებული გადაწყვეტილების გათვალისწინებით.

4. სამსახური უზრუნველყოფს პირველი თავის მე-8 მუხლის თითოეული პუნქტისა და ქვეპუნქტის მიხედვით განსაზღვრული მიმართულებებისთვის საჭირო ქმედებების განხორციელებას.

თავი II

ინფორმაციული უსაფრთხოების მართვის ორგანიზაციული სტრუქტურა

მუხლი 9. ინფორმაციული უსაფრთხოების მენეჯერი

ინფორმაციული უსაფრთხოების მენეჯერი ინიშნება სამსახურის უფროსის მიერ (სამსახურის უფროსის სამართლებრივი აქტის საფუძველზე) და მის მოვალეობაში შედის სამსახურში არსებული ინფორმაციული უსაფრთხოების საკითხების ყოველდღიური მონიტორინგი, პოლიტიკის მოთხოვნების შესრულების მონიტორინგი, ინფორმაციული აქტივების და მასზე წვდომის აღწერა, პოლიტიკის უზრუნველყოფისათვის საჭირო დოკუმენტაციის მომზადება, ინციდენტების შეგროვება და მათზე რეაგირების მონიტორინგი, ანგარიშების, სხდომების ოქმებისა და დღის

წესრიგის მომზადება. კომპეტენციის ფარგლებში, სამსახურის თანამშრომლებისთვის ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზებაში მონაწილეობა.

მუხლი 10. ინფორმაციული უსაფრთხოების შიდა აუდიტი

სამსახური ვალდებულია ჩაატაროს იუმს-ის აუდიტი დაგეგმილი პერიოდულობით და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები:

ა) შეესაბამება თუ არა სტანდარტის, საკანონმდებლო მოთხოვნებს;

ბ) შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება თუ არა მისი დანერგვა და მხარდაჭერა;

დ) ფუნქციონირებს თუ არა გეგმის შესაბამისად.

თავი III

განხორციელების ეტაპები

მუხლი 12. ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების ეტაპები

ინფორმაციული უსაფრთხოების პოლიტიკის დანერგვა განხორციელდება სამ ძირითად ეტაპად:

1. ინფორმაციული უსაფრთხოების პოლიტიკის დაგეგმვის ეტაპი - დაგეგმვის ეტაპზე უნდა განხორციელდეს:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის გავრცელების სფეროში არსებული ინფორმაციული აქტივების აღწერა და მათი შესაბამისი მფლობელების დადგენა;

ბ) აღრიცხული ინფორმაციული აქტივების რისკების ანალიზის და შეფასების ჩატარება, საფრთხეების იდენტიფიცირება და მათი აღმოფხვრის მიზნით სათანადო კონტროლის მექანიზმების შემუშავება/განსაზღვრა;

გ) დაგეგმვის პროცესის შედეგად შესაბამისი ქვე-პოლიტიკების, სახელმძღვანელო მითითებებისა და ინსტრუქციების შემუშავება.

2. ინფორმაციული უსაფრთხოების პოლიტიკის დანერგვის ეტაპი - დანერგვის ეტაპზე უნდა განხორციელდეს:

ა) დაგეგმვის ეტაპზე შერჩეული კონტროლის მექანიზმების დანერგვისათვის საჭირო, სათანადო მატერიალური და ფინანსური რესურსების უზრუნველყოფა, საფრთხეებთან დაკავშირებული ალბათობის ან/და უარყოფითი შედეგების შესამცირებლად;

ბ) დანერგვის პროცესში ჩართული პერსონალის კვალიფიკაციის ამაღლება ტრენინგების და სხვა ღონისძიებების ჩატარების გზით.

3. ინფორმაციული უსაფრთხოების პოლიტიკის მონიტორინგის და შესაბამისი კორექტივების შეტანის ეტაპი - მონიტორინგის და შესაბამისი კორექტივების შეტანის ეტაპზე უნდა განხორციელდეს:

ა) დანერგვის ეტაპის განხორციელების შედეგად დაგროვებული ჩანაწერების ანალიზი, ნაკლოვანებების გამოვლენა, შემდგომი კორექტირება კონტროლის არსებულ მექანიზმებში და სათანადო სახელმძღვანელო მითითებებში შესაბამისი ცვლილებების განხორციელება;

ბ) ინფორმაციული უსაფრთხოების მენეჯერი, თავისი უფლებამოსილებების ფარგლებში ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტურად ფუნქციონირების უზრუნველსაყოფად - განახორციელებს მონიტორინგს და მის შედეგებს წარუდგენს სამსახურის უფროსს. მონიტორინგის შედეგების მიხედვით რეგულარულად მოხდება ინფორმაციული უსაფრთხოების მართვის სისტემის გაუმჯობესება და განახლება;

გ) ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტურად ფუნქციონირების უზრუნველსაყოფად, დადგენილი პერიოდულობით ჩატარდება ინფორმაციული უსაფრთხოების მართვის სისტემის აუდიტი, კონტროლის მექანიზმების, პროცედურების და დოკუმენტაციის საკანონმდებლო და ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებთან შესაბამისობის მიზნით.

თავი IV

პასუხისმგებლობა ინფორმაციულ უსაფრთხოებაზე

მუხლი 12. ინფორმაციული უსაფრთხოების მმართველი სუბიექტები

1. სამსახურის ინფორმაციული უსაფრთხოების გავრცელების სფეროში შემავალი სტრუქტურული ქვე-დანაყოფების ხელმძღვანელები, მათი მოადგილე(ებ)ი, სამსახურის თანამშრომლები, ვალდებულნი არიან დაიცვან წინამდებარე პოლიტიკისა და აღნიშნულ სფეროში მოქმედი კანონმდებლობით განსაზღვრული სხვა მოთხოვნები, ხოლო ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევების გამოვლენის შემთხვევაში დროულად მოახდინონ ინფორმაციული უსაფრთხოების მენეჯერის ინფორმირება.

2. ინფორმაციული უსაფრთხოების პოლიტიკის დამტკიცებას ახორციელებს სამსახურის უფროსი ინდივიდუალურ-სამართლებრივი აქტით;

3. ინფორმაციული უსაფრთხოების მიმართულებით, შინა-სამსახურეობრივი წესების დამტკიცებას ახორციელებს სამსახურის უფროსი ინფორმაციული უსაფრთხოების მენეჯერის წარდგინების საფუძველზე;

4. ინფორმაციული უსაფრთხოების რისკების მართვის მეთოდოლოგიას ამტკიცებს სამსახურის უფროსი ბრძანებით, ხოლო ინფორმაციული უსაფრთხოების მიმართულებით რისკების მართვაზე გადაწყვეტილებების მიღებას ახორციელებს, ინფორმაციული უსაფრთხოების მენეჯერი;

5. ინფორმაციული უსაფრთხოების მიმართულებით რისკების მართვის კოორდინაციას და მისაღები გადაწყვეტილებების პროექტების მომზადებას, ახორციელებს ინფორმაციული უსაფრთხოების მენეჯერი;

6. ინფორმაციული უსაფრთხოების მიმართულებით რისკების გამოვლენას ახდენს, ინფორმაციული აქტივის მფლობელი;

7. ინფორმაციული უსაფრთხოების პოლიტიკისა და შინა-სამსახურეობრივი გამოყენების წესების პროექტს სამსახურის უფროსს წარუდგენს ინფორმაციული უსაფრთხოების მენეჯერი;

8. ინფორმაციული უსაფრთხოების გავრცელების სფეროში შემავალი დეპარტამენტების თანამშრომლები ვალდებულნი არიან დაიცვან ინფორმაციული უსაფრთხოების მიმართულებით დადგენილი მოთხოვნები;

9. ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების მონიტორინგს ახორციელებს ინფორმაციული უსაფრთხოების მენეჯერი;

10. ადმინისტრაციული დეპარტამენტი უზრუნველყოფს ახლად აყვანილი თანამშრომლებისათვის, ინფორმაციული უსაფრთხოების მიმართულებით არსებული შინა-სამსახურეობრივი დოკუმენტაციის (პროცედურების) გაცნობას, ხოლო თანამშრომელთა ცნობიერების ამაღლებისათვის აუცილებელი სატრენინგო მოდულების შემუშავებას და განხორციელებას უზრუნველყოფს ინფორმაციული უსაფრთხოების მენეჯერი.

მუხლი 13. ინფორმაციული უსაფრთხოების პოლიტიკის მართვა და განახლება

1. ინფორმაციული უსაფრთხოების პოლიტიკის განხილვისა და გაუმჯობესების საფუძველს შესაძლოა წარმოადგენდეს:

ა) დაწესებულების ორგანიზაციულ-სტრუქტურული ცვლილება;

ბ) ტექნოლოგიური ცვლილება;

გ) ცვლილება საქმიანობის მიზნებსა და პროცესებში;

დ) ახლადაღმოჩენილი სისუსტეები და საფრთხეები;

ე) დანერგილი კონტროლის მექანიზმების ეფექტიანობის ცვლილება;

ვ) საკანონმდებლო ცვლილებები;

ზ) ახლად გამოვლენილი რისკები, რომლებმაც შესაძლოა უარყოფითი გავლენა იქონიონ ორგანიზაციის ძირითად საქმიანობაზე.

2. ინფორმაციული უსაფრთხოების ეფექტურობის უზრუნველსაყოფად, გამოიყენება მუდმივ გაუმჯობესებაზე ორიენტირებული მიდგომა, რაც გულისხმობს: დაგეგმარების, შესრულების, შემოწმებისა და გაუმჯობესების მუდმივ ციკლს.

3. ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტის გეგმიური განხილვა უნდა განხორციელდეს საჭიროებისამებრ, მაგრამ არანაკლებ წელიწადში ერთხელ ინფორმაციული უსაფრთხოების მენეჯერის მიერ.

4. ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტის განახლება მოხდება 6 თვის პერიოდულობით, სამსახურის საჭიროების, მიზნების, უსაფრთხოების მოთხოვნების და არსებული პროცესების გათვალისწინებით.

დანართი N2

სსიპ - საფინანსო-ანალიტიკური სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემების გავრცელების სფერო

მუხლი 1. ინფორმაციული უსაფრთხოების გავრცელების სფეროს განსაზღვრის მიზანი

1. ინფორმაციული უსაფრთხოების გავრცელების სფეროს დოკუმენტის მიზანია, ნათლად განსაზღვროს სსიპ - საფინანსო-ანალიტიკურ სამსახურში (შემდგომში - სამსახური) ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლები.

2. სამსახურში ჩამოყალიბდა და განისაზღვრა გავრცელების სფერო და საზღვრები, ინფორმაციული უსაფრთხოების მართვის სისტემასთან მიმართებით მგს 27001:2011 პუნქტი 4.2.1 ,,ა“-ს თანახმად.

მუხლი 2. ორგანიზაციის სტრუქტურა

1. სამსახურის სტრუქტურა შედგება შემდეგი სტრუქტურული ქვედანაყოფებიდან:

ა) ადმინისტრაციული დეპარტამენტი;

ბ) კვლევის და სისტემური ანალიზის დეპარტამენტი;

გ) პროგრამული უზრუნველყოფის დეპარტამენტი;

დ) სისტემური ადმინისტრირების დეპარტამენტი;

ე) საოპერაციო დეპარტამენტი;

ვ) ვებრესურსების მართვის დეპარტამენტი.

მუხლი 3. გავრცელების სფერო

სამსახურის ხელმძღვანელობის გადაწყვეტილებით, ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა, მიზანშეწონილია სამსახურის ყველა სტრუქტურულ ერთეულში, ვინაიდან ყველა დეპარტამენტის ინფორმაციული აქტივების არასათანადო დაცვამ, შესაძლოა გამოიწვიოს სამსახურის საქმიანობის შეჩერება.

მუხლი 4. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტის მოქმედების სფერო, კონტროლი და კანონიერება

1. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტის განხილვა განხორციელდეს არანაკლებ წელიწადში ერთხელ სამსახურის საჭიროებების, მიზნების, უსაფრთხოების მოთხოვნების, არსებული პროცესების გათვალისწინებით და ასევე, იმ საორგანიზაციო ცვლილებების გათვალისწინებით, რაც გავლენას იქონიებს ინფორმაციული უსაფრთხოების მართვის სისტემაზე

2. აღნიშნული დოკუმენტი ვრცელდება სამსახურის გავრცელების სფეროში შემავალ სტრუქტურულ ქვედანაყოფებში არსებულ ყველა აქტივზე, თანამშრომლებსა და მესამე პირებზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტთან დაკავშირებულნი არიან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობებით და რომლებიც უზრუნველყოფენ ინფორმაციული აქტივის წვდომას ასეთი ურთიერთობების ფარგლებში.