პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

1. შესავალი

პერსონალურ მონაცემთა დაცვის სამსახური (შემდგომ - სამსახური) დამოუკიდებელი სახელმწიფო ორგანოა, რომლის საქმიანობის მიმართულებებია:

ა) პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი;

ბ) 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 საქმიანობაში უსაფრთხოების, მათ შორის, ინფორმაციული უსაფრთხოების სტანდარტების დანერგვას არსებითი მნიშვნელობა აქვს სამსახურის საქმიანობის უზრუნველსაყოფად, ასევე, მოქალაქეთა ინტერესების დასაცავად.

სამსახურში ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, დანერგილია კრიტიკული ინფორმაციული სისტემებისა და საკომუნიკაციო სისტემების კიბერსაფრთხეებისაგან დაცვის არაერთი მექანიზმი.

შესაბამისად, სამსახურის ხელმძღვანელობის განცხადებულ და განგრძობად პრიორიტეტს წარმოადგენს სამსახურის საქმიანობაში უსაფრთხოების, მათ შორის, ინფორმაციული უსაფრთხოების ეროვნული და საერთაშორისო სტანდარტებისა და წესების დანერგვა, ასევე, ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების მუდმივი გაუმჯობესება.

სამსახურის ხელმძღვანელობა აცნობიერებს, რომ უსაფრთხოების, განსაკუთრებით კი, ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, მნიშვნელოვანია რისკების შეფასებაზე დაფუძნებული მიდგომების გამოყენება სამსახურის საქმიანობის პროცესებში, მათ შორის, ინფორმაციული უსაფრთხოების მართვის სისტემაში.

2. რეგულირების სფერო

ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს განსაზღვრის მიზანია სამსახურის ყველა კრიტიკული ინფორმაციული სისტემის, ინფორმაციული აქტივის, პროცესის, ტექნოლოგიის, პროდუქტის/სერვისის, მისი ორგანიზაციული სტრუქტურისა და ადგილმდებარეობის განსაზღვრა, რომლებზეც უნდა გავრცელდეს ინფორმაციული უსაფრთხოების მართვის სისტემისთვის დადგენილი მოთხოვნები.

3. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს განსაზღვრის პრინციპები

ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს განსაზღვრისას სამსახურმა გაითვალისწინა:
ა) სამსახურის მიზნები;
ბ) სამსახურის საქმიანობის პროცესები;

გ) ორგანიზაციული კონტექსტი და გარემო ფაქტორები, რომლებიც მნიშვნელოვანია სამსახურის მიზნებისთვის და გავლენას ახდენენ ინფორმაციული უსაფრთხოების მართვის სისტემისათვის დასახული შედეგების მიღწევაზე;
დ) ინფორმაციული უსაფრთხოების მართვის სისტემისთვის მნიშვნელოვანი დაინტერესებული მხარეები, მათი მოთხოვნები და მოლოდინები, რაც მოიცავს როგორც საკანონმდებლო მოთხოვნებს, ასევე სახელშეკრულებო ხასიათის ვალდებულებებს;
ე) ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნები.

4. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

4.1. სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემა ვრცელდება სამსახურის საქმიანობის შემდეგ პროცესებზე და აქტივებზე:

ა) პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი:
- მოქალაქეთა განცხადებების და შეტყობინებების დამუშავების პროცესი - ფიზიკური ან იურიდიული პირის მიერ, განცხადების ან შეტყობინების საფუძველზე საქმის შესწავლა და შესაბამისი მოქმედებების ჩატარება;
- პერსონალურ მონაცემთა დამუშავების კანონიერების შესწავლის (ინსპექტირების) პროცესი - მონაცემთა დამმუშავებლის გეგმური ან არაგეგმური შემოწმება;
- კონსულტაციის პროცესი - ფიზიკური და იურიდიული პირების კონსულტაცია;
- პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემის ნებართვის გაცემის პროცესი - ქვეყნის გარეთ გადასაცემ მონაცემებზე ნებართვის გაცემა;
- სამართალშემოქმედებითი პროცესი;
- სამსახურში ადმინისტრაციული წარმოების პროცესი;
- სავარაუდო დანაშაულის შესახებ უფლებამოსილი ორგანოსთვის შეტყობინების პროცესი - საქმიანობის პროცესში დანაშაულის ნიშნების აღმოჩენის შეტყობინება უფლებამოსილი სახელმწიფო ორგანოსთვის.

ბ) სამსახურის ყველა თანამშრომელზე, სტაჟიორზე და სტრუქტურულ ერთეულზე;
გ) სამსახურის საკუთრებაში არსებულ ყველა იმ შენობაზე და შენობის ნაწილზე, რომელშიც წარიმართება ამ პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული პროცესები და აღნიშნულის ფარგლებში ხორციელდება ინფორმაციის დამუშავება ან/და განთავსებულია ინფორმაციის დამუშავების საშუალებები.
4.2. სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემა არ ვრცელდება სამსახურის საქმიანობის შემდეგ პროცესებზე და აქტივებზე:
ა) სახელმწიფო საიდუმლოებას მიკუთვნებულ საქმიანობაზე;
ბ) ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლზე;
გ) სამსახურის საკუთრებაში არსებულ ყველა იმ შენობაზე და შენობის ნაწილზე, რომელშიც წარიმართება ამ პუნქტის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული პროცესები და აღნიშნულის ფარგლებში ხორციელდება ინფორმაციის დამუშავება ან/და განთავსებულია ინფორმაციის დამუშავების საშუალებები.

5. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს გადახედვა

სამსახურის ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს გადახედვის საფუძველი შეიძლება გახდეს:
ა) სამსახურში განხორციელებული მნიშვნელოვანი ორგანიზაციული/ტექნიკური ცვლილებები;
ბ) ინფორმაციული უსაფრთხოების სფეროში არსებული ნორმატიული აქტების ცვლილებები;
გ) შიდა აუდიტის/გარე აუდიტის შედეგები;
დ) სხვა გარემოებები, რომლებიც უკავშირდება სამსახურის ინფორმაციულ აქტივებს ან/და ინფორმაციული აქტივების დამუშავების საშუალებებს;
ე) ინფორმაციული უსაფრთხოების მენეჯერის ინიციატივა.