საქართველოს საარჩევნო ადმინისტრაციის

ინფორმაციული უსაფრთხოების პოლიტიკა

ცესკო
საქართველოს საარჩევნო ადმინისტრაცია

საქართველოს ცენტრალური საარჩევნო კომისია

+995 32 251 00 51
დ. აღმაშენებლის ხეივანი მე-13 კმ.
WWW.CESKO.GE

მუხლი 1. შესავალი

1. საქართველოს საარჩევნო ადმინისტრაციის მისიაა, თავისუფალი, სამართლიანი, სანდო და გამჭვირვალე არჩევნების ჩატარების გზით, ხელი შეუწყოს დემოკრატიული საზოგადოების მშენებლობასა და გაძლიერებას.
2. საქართველოს საარჩევნო ადმინისტრაცია აცნობიერებს, რომ აღნიშნული მიზნის მიღწევა საჭიროებს საარჩევნო პროცესებში მიღებული ინფორმაციის, სანდო და ეფექტური საშუალებებით დამუშავებას, რაც გულისხმობს თანამედროვე, დახვეწილი და უსაფრთხო ინფორმაციული ტექნოლოგიების გამოყენებას; ეს უკანასკნელი კი ხელს შეუწყობს და კიდევ უფრო აამაღლებს საარჩევნო ადინისტრაციის მიერ საკუთარი უფლებამოსილებების განხორციელებისას დასამუშავებელი ინფრომაციის მთლიანობის, კონფიდენციალურობის და ხელმისაწვდომობის ხარისხის ამაღლებას.
3. საქართველოს საარჩევნო ადმინისტრაციის მისიისა და მიზნების წარმატებულად შესრულებისთვის, განსაკუთრებით მნიშვნელოვანია ორგანიზაციის საქმიანობის ამა თუ იმ მიმართულებაში ჩართული ინფორმაციული აქტივების უსაფრთხოების სათანადო დონის უზრუნველყოფა. საქართველოს საარჩევნო ადმინისტრაციის საქმია-ნობა დაკავშირებულია ინფორმაციის დამუშავება-შენახვასთან, როგორც ელექტრონული ისე არაელექტრონული სახით. შესაბამისად, მნიშვნელოვანია აღნიშნული ინფორმაციის სათანადო დონეზე დაცვა.
4. ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანია: ხელი შეუწყოს საარჩევნო ადმინისტრაციას ინფორმაციის ხელმისაწვდომობის, მთლიანობისა და კონფიდენციალურობის სათანადო ხარისხის უზრუნველყოფაში, ინფორმაციული უსაფრთხოების პოლიტიკის გავრცელების სფეროში ისეთი პროცესების ჩამოყალიბებაში, რაც ერთის მხრივ გამოავლენს ინფორმაციული უსაფრთხოების კუთხით არსებულ ხარვეზებს, ხოლო მეორეს მხრივ, გააუმჯობესებს ინფორმაციული აქტივების დამუშავებისათვის განკუთვნილი პროცესების დაგეგმარების, შესრულებისა და შემოწმების პროცესს.
5. ინფორმაციული უსაფრთხოების მართვის სისტემა ხელს შეუწყობს ორგანიზაციის მიერ დამუშავებული ინფორმაციის სანდოობის ხარისხის ამაღლებას.

მუხლი 2. ტერმინთა განმარტებები

ამ დოკუმენტისთვის გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

1. საქართველოს საარჩევნო ადმინისტრაცია — ცესკო და მისი აპარატი, საოლქო საარჩევნო კომისიები, სსიპ — საარჩევნო სისტემების განვითარების, რეფორმებისა და სწავლების ცენტრი;
2. ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) — სისტემა, რომელიც უზრუნველყოფს ინფორმაციული უსაფრთხოების დანერგვას, ფუნქციონირებას, მონიტორინგს, განხილვას, მხარდაჭერას და გაუმჯობესებას;
3. ინფორმაციული უსაფრთხოება — ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შენარჩუნება და დაცვა;
4. ინფორმაციული უსაფრთხოების პოლიტიკა — საქართველოს საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების მართვის სისტემის, აგრეთვე პოლიტიკის ძირითადი დოკუმენტისა და მასთან დაკავშირებული ინსტრუქციების და სახელმძღვანელო მითითებების ერთობლიობა;
5. 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;
6. კონტროლის მექანიზმი — ინფორმაციული უსაფრთხოების მართვის სახელმძღვანელო პრინციპები, მიმართული საფრთხესთან დაკავშირებული ალბათობის ან/და უარყოფითი შედეგების შესამცირებლად.
7. კრიტიკული ინფორმაციული სისტემის სუბიექტი — „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის თანამხად, საქართველოს მთავრობის დადგენილებით განსაზღვრული სახელმწიფო ორგანო — საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი;
8. ხელმისაწვდომობა — კრიტიკულ ინფორმაციაზე წვდომისა და გამოყენებადობის შესაძლებლობა ავტორიზებული სუბიექტის მიერ.
9. მთლიანობა — აქტივის სიზუსტისა და სისრულის მახასიათებელი თვისება;

10. კონფიდენციალურობა — ინფორმაციის მახასიათებელი, რაც გულისხმობს მხოლოდ ავტორიზებული სუბიექტისთვის ინფორმაციის ხელმისაწვდომობას.
11. რისკებთან მოპყრობა — რისკის დაშვება, რისკის აცილება პროცესზე უარის თქმით, რისკის შემცირება კონტროლის მექანიზმების დანერგვით და მესამე მხარეზე გადაცემა/დაზღვევა;
12. საბჭო — ინფორმაციული უსაფრთხოების საბჭო, ინფორმაციული უსაფრთხოების მიმართულებით, პოლიტიკისა და შინასამსახურებრივი დოკუმენტაციის შემუშავების მიზნით, ცესკოს წევრების, აპარატის სტრუქტურული ერთეულების ხელმძღვანელებისაგან და სსიპ საარჩევნო სისტემების განვითარების, რეფორმებისა და სწავლების ცენტრის წარმომადგენლისაგან შემდგარი სამუშაო ჯგუფი, რომლის შემედგენლობა და უფლებამოსილებები განისაზღვრება ცესკოს თავმჯდომარის ბრძანებით;
13. 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.

მუხლი 3. საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების ნორმატიული საფუძვლები

1. ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-4 მუხლის პირველი პუნქტის შესაბამისად, „კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 29 აპრილის N312 დადგენილების თანახმად, საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი შეტანილია კრიტიკული ინფორმაციული სისტემის სუბიექტთა ნუსხაში.
2. საარჩევნო ადმინისტრაცია 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.

მუხლი 4. საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების პოლიტიკის მიზანი

საარჩევნო ადმინისტრაცია გამოხატავს ურყევ ნებას დანერგოს 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. საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

საქართველოს საარჩევნო ადმინისტრაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო განსაზღვრულია დანართი1–ის შესაბამისად.

მუხლი 6. ინფორმაციული უსაფრთხოების პოლიტიკის ძირითადი მიმართულებები

1. საარჩევნო ადმინისტრაცია (მათ შორის ცესკოს აპარატი) 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 დოკუმეტების მეშვეობით, უზრუნველყოფს ტექნიკური საშუალებების გამართულად ფუნქციონირებას და ინფორმაციული აქტივების მთლიანობას, ხელმისაწვდომობასა და კონფიდენციალურობას. აღნიშნული მიზნის მისაღწევად გამოიყოფა შემდეგი მიმართულებები:

ა) ინფორმაციული უსაფრთხოების მართვის სისტემის შექმნა – მოიცავს:

ა.ა) ინფორმაციული უსაფრთხოების მართვის სისტემის შექმნას;

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

ა.გ) პასუხისმგებლობათა გადანაწილებას ინფორმაციული აქტივების მფლობელ პირებზე, გარე უსაფრთხოებას – მესამე პირებთან, მომხმარებლებთან ურთიერთობა.

ბ) ინფორმაციული აქტივების მართვა – მოიცავს:

ბ.ა) ინფორმაციული აქტივების აღწერას;

ბ.ბ) აქტივების მფლობელების იდენტიფიცირებასა და აქტივების კლასიფიკაციას.

გ) ინფორმაციული უსაფრთხოების რისკების მართვა – მოიცავს:

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

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

დ) ადამიანური რესურსების უსაფრთხოება – მოიცავს:

დ.ა) სამუშაო პირობებს;

დ.ბ) სამსახურებრივი ფუნქციების განხორციელების დაწყება/შეწყვეტას;

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

ე) ფიზიკური უსაფრთხოება და გარემო პირობების უსაფრთხოება – მოიცავს:

ე.ა) ფიზიკური უსაფრთხოების პარამეტრებს;

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

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

ვ) კომუნიკაციებისა და ოპერაციების მართვა – მოიცავს:

ვ.ა) საოპერაციო პროცედურებს და პასუხისმგებლობის გადანაწილებას;

ვ.ბ) მესამე მხარის მიერ შემოთავაზებული სერვისების მართვას;

ვ.გ) სისტემის დაგეგმვას და მართვას;

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

ვ.ე) ინფორმაციის მედია–მატარებლების მართვას და მონიტორინგს.

ზ) წვდომის კონტროლის მართვა – მოიცავს:

ზ.ა) მომხმარებელთა წვდომის მართვას და შესაბამის პასუხიმგელობას;

ზ.ბ) ქსელურ რესურსებზე წვდომის კონტროლის;

ზ.გ) ოპერაციულ სისტემებზე წვდომის კონტროლს;

ზ.დ) პროგრამებსა და ინფორმაციაზე წვდომის კონტროლს, მობილურ ტექნოლოგიებს და დისტანციურ მუშაობას.

თ) ინფორმაციული აქტივების დაცვა – მოიცავს:

თ.ა) ორგანიზაციული ჩანაწერებისა და მონაცემების დაცვას;

თ.ბ) პერსონალური მონაცემების შემცველი ინფორმაციის დაცვას;

თ.გ) 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 სუბიექტისათვის.

ი) ინფორმაციული სისტემების შეძენა, შემუშავება 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) ინფორმაციული უსაფრთხოების ინციდენტების მართვა – მოიცავს:

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

კ.ბ) ინფორმაციული უსაფრთხოების ინციდენტებისა და გაუმჯობესებების მართვას.

მუხლი 7. ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების ეტაპები

1. ინფორმაციული უსაფრთხოების პოლიტიკის დაგეგმვის ეტაპი – დაგეგმვის ეტაპზე უნდა გახორციელდეს:

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

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

გ) დაგეგმვის პროცესის შედეგად შესაბამისი 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 რესურსის უზრუნველყოფა, საფრთხესთან 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 მართვის სისტემის ეფექტურად ფუნქციონირების უზრუნველსაყოფად ინფორმაციული უსაფრთხოების მენეჯერი განახორციელებს მონიტორინგს და მის შედეგებს წარუდგენს ცესკოს თავმჯდომარეს. 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 მოთხოვნებთან შესაბამისობის მიზნით.

მუხლი 8. ინფორმაციული უსაფრთხოების მმართველი სუბიექტები

1. ინფორმაციული უსაფრთხოების პოლიტიკის დამტკიცებას ახორციელებს ცესკო განკარგულებით.
2. ინფორმაციული უსაფრთხოების მიმართულებით, შინასამსახურებრივი წესების დამტკიცებას ახორციელებს ცესკოს თავმჯდომარე ინფორმაციული უსაფრთხოების საბჭოს წარდგინების საფუძველზე.
3. ინფორმაციული უსაფრთხოების მიმართულებით რისკების მართვაზე გადაწყვეტილებების მიღებას ახორციელებს, ინფორმაციული უსაფრთხოების საბჭო.
4. ინფორმაციული უსაფრთხოების მიმართულებით რისკების მართვის კოორდინაციას, მათ შორის საბჭოს მიერ მისაღები გადაწყვეტილებების პროექტების მომზადებას, ახორციელებს, ინფორმაციული უსაფრთხოების მენეჯერი.

5. ინფორმაციული უსაფრთხოების მიმართულებით რისკების გამოვლენას ახდენს, ინფორმაციული აქტივის მფლობელი.
6. ინფორმაციული უსაფრთხოების პოლიტიკისა და შინასამსახურებრივი გამოყენების წესების პროექტს საბჭოს წარუდგენს ინფორმაციული უსაფრთხოების მენეჯერი.
7. ინფორმაციული უსაფრთხოების გავრცელების სფეროში შემავალი სტრუქტურული ერთეულის ხელმძღვანელი პირები, ვალდებულნი არიან აკონტროლონ მათ დაქვემდებარებაში მყოფი თანამშრომლების მიერ ინფორმაციული უსაფრთხოების მოთხოვნების შესრულება, ასევე ინფორმაციული უსაფრთხოების მოთხოვნების დარღვევების გამოვლენის შემთხვევაში უზრუნველყონ ინფორმაციული უსაფრთხოების მენეჯერის ინფორმირება.
8. ინფორმაციული უსაფრთხოების გავრცელების სფეროში შემავალი სამსახურების თანამშრომლები ვალდებულნი არიან დაიცვან ინფორმაციული უსაფრთხოების მიმართულებით დადგენილი მოთხოვნები.
9. ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების მონიტორინგს ახორციელებს ინფორმაციული უსაფრთხოების მენეჯერი.
10. ადამიანური რესურსების მართვის სამსახური უზრუნველყოფს ახლადაყვანილი თანამშრომლებისათვის, ინფორმაციული უსაფრთხოების მიმართულებით არსებული შინასამსახურებრივი დოკუმენტაციის (პროცედურების) გაცნობას, ხოლო თანამშრომელთა ცნობიერების ამაღალებისათვის აუცილებელი სატრენინგო მოდულების შემუშავებას და განხორციელებას უზრუნველყოფს ინფორმაციული უსაფრთხოების მენეჯერი.

მუხლი 9. 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 საფრთხეები;
ე) დანერგილი კონტროლის მექანიზმების ეფექტიანობის ცვლილება;
ვ) საკანონმდებლო ცვლილებები;
ზ) ახლად აღმოჩენილი 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 საბჭოს მიერ.

დანართი 1

საქართველოს საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

მუხლი 1. ინფორმაციული უსაფრთხოების გავრცელების სფეროს განსაზღვრის მიზანი

ინფორმაციული უსაფრთხოების გავრცელების სფეროს დოკუმენტის მიზანია ნათლად განსაზღვროს საქართველოს საარჩევნო ადმინისტრაციის ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლები.

მუხლი 2. საარჩევნო ადმინისტრაციის სტრუქტურა

1. საარჩევნო ადმინისტრაციის სტრუქტურა შედგება შემდეგი ერთეულებისაგან:

ა) ცენტრალური საარჩევნო კომისია და მისი აპარატი; ცენტრალური საარჩევნო კომისიის აპარატში შექმნილია და ფუნქციონირებს შემდეგი სტრუქტურული ერთეულები:

ა.ა) საარჩევნო პროცესების მართვის დეპარტამენტი;
ა.ბ) იურიდიული დეპარტამენტი;
ა.გ) სარეგისტრაციო და ადმინისტრაციული დეპარტამენტი;
ა.დ) საზოგადოებასთან ურთიერთობის დეპარტამენტი;
ა.ე) საფინანსო დეპარტამენტი;
ა.ვ) საინფორმაციო ტექნოლოგიების დეპარტამენტი;
ა.ზ) კოორდინაციის, დაგეგმვისა და ანგარიშგების დეპარტამენტი;
ა.თ) ადამიანური რესურსების მართვის სამსახური;
ა.ი) შიდა აუდიტის სამსახური;

ბ) საოლქო და საუბნო საარჩევნო კომისიები;

გ) სსიპ — საარჩევნო სისტემების განვითარების, რეფორმებისა და სწავლების ცენტრი.

მუხლი 3. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო

ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა, თავდაპირველ ეტაპზე მიზანშეწონილია ამომრჩეველთა ერთიანი სიის ფორმირების; არჩევნების შედეგების შეჯამების, არჩევნების შედეგების გასაჯაროვების; საჯარო ინფორმაციის გამოქვეყნების; საარჩევნო ადმინისტრაციის მოხელეთა სერთიფიცირების პროცესის; საარჩევნო სუბიექტების არჩევნებში მონაწილეობის მიღების უფლების მიზნით საარჩევნო რეგისტრაციის პროცესისა და ელექტრონული ინფორმაციის ადმინისტრირების პროცესებისთვის, საარჩევნო ადმინისტრაციის ქვემოჩამოთვლილ სტრუქტურულ ერთეულებში:

1) ცენტრალური საარჩევნო კომისიის აპარატი:
   ა) საარჩევნო პროცესების მართვის დეპარტამენტი;
   ბ) საზოგადოებასთან ურთიერთობის დეპარტამენტი;
   გ) სარეგისტრაციო და ადმინისტრაციული დეპარტამენტი;
   დ) საინფორმაციო ტექნოლოგიების დეპარტამენტი.
2) სსიპ — საარჩევნო სისტემების განვითარების, რეფორმებისა და სწავლების ცენტრი;
3) საოლქო საარჩევნო კომისიები.

შენიშვნა:

1. ზემოჩამოთვლილ სტრუქტურულ ერთეულებში არსებული ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფამ შესაძლოა გამოიწვიოს საარჩევნო ადმინისტრაციის ფუნქციებისათვის მნიშვნელოვანი ზიანი.
2. ზემოჩამოთვლილი სტრუქტურული ერთეულები უზრუნველყოფენ, როგორც ცესკოს საქმიანობის ძირითადი მიმართულებების ოპერირებას, ისე დამხმარე სერვისების მიწოდებას, ამ პროცესებში არსებული ინფორმაციის ტექნოლოგიურ დამუშავებასა და საზოგადოებისათვის ხელმისაწვდომობას. ზემოჩამოთვლილი სტრუქტურული ერთეულების ეფექტურად და გამართულად მუშაობისთვის საჭიროა ინფორმაციული აქტივების მუდმივი მონიტორინგი, რისკების და საფრთხეების პრევენციისათვის სათანადო ქმედებების გატარება.

3. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროში განსაკუთრებული მნიშვნელობა ენიჭება საინფორმაციო ტექნოლოგიების დეპარტამენტს, რადგანაც იგი უზრუნველყოფს:

ა) ცესკოში საინფორმაციო ტექნოლოგიების დანერგვას, მის განახლებას და გამართულ ფუნქციონირებას;

ბ) ლოკალური და გლობალური ქსელური კავშირების შექმნას და მათ მდგრად მუშაობას;

გ) საინფორმაციო ტექნოლოგიებთან დაკავშირებული პოტენციური რისკის გამოვლენას;

დ) საქართველოს საარჩევნო ადმინისტრაციის თანამშრომელთა სამუშაო ადგილების (პერიფერიული მოწყობილობები, პროგრამული უზრუნველყოფა და საკომუნიკაციო საშუალება) გამართვას და მდგრად მუშაობას;

ე) იქიდან გამომდინარე, რომ იუმს–ის გავრცელების სფეროში შემავალ სტრუქტურულ ერთეულებში არსებული ინფორმაციული აქტივები მნიშვნელოვანია საარჩევნო ადმინისტრაციისთვის და მათი დამუშავება ძირითადად ხორციელდება ინფორმაციული ტექნოლოგიების გამოყენებით, საინფორმაციო ტექნოლოგიების დეპარტამენტი იქნება ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვის გარანტი. საინფორმაციო ტექნოლოგიების დეპარტამენტი უზრუნველყოფს კრიტიკული ინფორმაციული სისტემის დაცულობას, ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისად, რომლის უწყვეტი ფუნქციონირებაც საარჩევნო ადმინისტრაციისათვის კრიტიკულ მნიშვნელობას წარმოადგენს.

მუხლი 4. იუმს-ის გავრცელების სფეროს გამონაკლისები

ცესკოს ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა მოცემულ ეტაპზე არ არის მიზანშეწონილი გავრცელების სფეროს გარეთ დარჩენილ სტრუქტურულ ერთეულებზე. იმის მიუხედავად, რომ აღნიშნული სტრუქტურული ერთეულები საქართველოს საარჩევნო ადმინისტრაციის ეფექტურ მუშაობას მნიშვნელოვნად უწყობენ ხელს, მათ დამუშავებაში არსებული ინფორმაციული აქტივი საარჩევნო ადმინისტრაციის ფუნქციებისათვის მოცემული ეტეპისათვის კრიტიკულს არ წარმოადგენს.

მუხლი 5. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტის მოქმედების სფერო და კონტროლი

1. ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფეროს დოკუმენტის განახლება მოხდება 6 თვის პერიოდულობით ცესკოს საჭიროებების, მიზნების, უსაფრთხოების მოთხოვნების, არსებული პროცესების გათვალისწინებით და ასევე, იმ საორგანიზაციო ცვლილებების გათვალისწინებით, რაც გავლენას იქონიებს ინფორმაციული უსაფრთხოების მართვის სისტემაზე.
2. აღნიშნული დოკუმენტი ვრცელდება საქართველოს საარჩევნო ადმინისტრაციის იუმს-ის გავრცელების სფეროში შემავალ სტრუქტურულ ერთეულებში 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.