საქართველოს სტანდარტი

სსკ 03.100.70; 35.030

ინფორმაციის უსაფრთხოება, კიბერუსაფრთხოება და საიდუმლოების დაცვა - ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემები - მოთხოვნები

საინფორმაციო მონაცემები

1 შემოტანილია: სსიპ - საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს სტანდარტების დეპარტამენტის მიერ.

განხილულია სტანდარტიზაციის ტექნიკური კომიტეტის, ტკ 2-ის „მენეჯმენტი და შესაბამისობის შეფასება“ მიერ.

2 მიღებულია: სსიპ - საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს გენერალური დირექტორის 27/12/2023 წლის №107 განკარგულებით სტანდარტიზაციის ტექნიკური კომიტეტის ტკ 2-ის „მენეჯმენტი და შესაბამისობის შეფასება“გადაწყვეტილების საფუძველზე.

3 წინამდებარე სტანდარტი წარმოადგენს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ისო-ს) სტანდარტის ისო 27001:2022 „ინფორმაციის უსაფრთხოება, კიბერუსაფრთხოება და სადუმლოების დაცვა - ინფორმაციის უსართხოების მენეჯმენტის სისტემები - მოთხოვნები“ იდენტურ თარგმანს (IDT).

4 პირველად

5 რეგისტრირებულია: სსიპ - საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს საქართველოს სტანდარტების რეესტრში 27/12/2023 წლის №268-1.1-00494

II

სარჩევი

წინასიტყვაობა V
შესავალი VI
1 გამოყენების სფერო 1
2 ნორმატიული მითითებები 1
3 ტერმინები და განმარტებები 1
4 ორგანიზაციის კონტექსტი 2
4.1 ორგანიზაციისა და მისი კონტექსტის გააზრება 2
4.2 დაინტერესებული მხარეების საჭიროებებისა და მოლოდინების გააზრება 2
4.3 ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის სფეროს განსაზღვრა 2
4.4 ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემა 2
5 ხელმძღვანელობა 3
5.1 ხელმძღვანელობა და ვალდებულება 3
5.2 პოლიტიკა 3
5.3 ორგანიზაციული როლები, პასუხისმგებლობა და უფლებამოსილება 4
6 დაგეგმვა 4
6.1 ღონისძიებები რისკებისა და შესაძლებლობების გადასაჭრელად 4
6.1.1 ზოგადი 4
6.1.2 ინფორმაციის უსაფრთხოების რისკის შეფასება 5
6.1.3 ინფორმაციის უსაფრთხოების რისკის დამუშავება 5
6.2 ინფორმაციის უსაფრთხოების მიზნები და მათი მიღწევის დაგეგმვა 6
6.3 ცვლილებების დაგეგმვა 7
7 მხარდაჭერა 7
7.1 რესურსები 7
7.2 კომპეტენცია 7
7.3 ცნობადობა 7
7.4 კომუნიკაცია 8
7.5 დოკუმენტირებული ინფორმაცია 8
7.5.1 ზოგადი 8
7.5.2 შექმნა და განახლება 8
7.5.3 დოკუმენტირებული ინფორმაციის კონტროლი 8
8 ექსპლუატაცია 9
8.1 საექსპლუატაციო დაგეგმვა და კონტროლი 9

8.2 ინფორმაციის უსაფრთხოების რისკის შეფასება 10
8.3 ინფორმაციის უსაფრთხოების რისკის მართვა 10
9 ეფექტურობის შეფასება 10
9.1 მონიტორინგი, გაზომვა, ანალიზი და შეფასება 10
9.2 შიდა აუდიტი 10
9.2.1 ზოგადი 10
9.2.2 შიდა აუდიტის პროგრამა 11
9.3 მენეჯმენტის ანალიზი 11
9.3.1 ზოგადი 11
9.3.2 მენეჯმენტის ანალიზის მონაცემები 11
9.3.3 მენეჯმენტის ანალიზის შედეგები 12
10 გაუმჯობესება 12
10.1 უწყვეტი გაუმჯობესება 12
10.2 შეუსაბამობა და მაკორექტირებელი მოქმედება 12

დანართი A (ნორმატიული) ინფორმაციის უსაფრთხოების კონტროლის ცნობარი 13
ბიბლიოგრაფია 23

წინასიტყვაობა

ისო (სტანდარტიზაციის საერთაშორისო ორგანიზაცია) და იეკ (საერთაშორისო ელექტროტექნიკური კომისია) ქმნიან მსოფლიო სტანდარტიზაციის სპეციალიზებულ სისტემას. ეროვნული ორგანოები, რომლებიც ისო-ს ან იეკ-ის წევრები არიან, შეიმუშავებენ საერთაშორისო სტანდარტებს შესაბამისი ორგანიზაციის მიერ შექმნილი ტექნიკურ კომიტეტებან ერთად, რომლებიც დაკავშირებულია ტექნიკური საქმიანობის კონკრეტულ სფეროებთან. ისოსა და იეკის ტექნიკური კომიტეტები თანამშრომლობენ იმ სფეროში, რომლებიც ორივე მხარისათვის ინტერესების სფეროს წარმოადგენს. ამ სამუშაოში მონაწილეობას იღებენ ისოსა და იეკთან დაკავშირებული სამთავრობო და არასამთავრობო საერთაშორისო ორგანიზაციები.

წინამდებარე სტანდარტის შესამუშავებლად საჭირო და მისი შემდგომი გამოყენებისათვის განკუთვნილი მეთოდები აღწერილია ისოსა და იეკის დირექტივებში (ნაწილი 1). კერძოდ, უნდა აღინიშნოს დამტკიცების კრიტერიუმები, რომლებიც აუცილებელია ისოს სხვადასხვა ტიპის დოკუმენტებისთვის. წინამდებარე დოკუმენტი შედგენილია ისოსა და იეკის დირექტივების მე-2 ნაწილის სარედაქციო წესების შესაბამისად (იხილეთ, www.iso.org/directives ან www.iec.ch/members_experts/refdocs).

აღსანიშნავია, რომ შესაძლოა მოცემული დოკუმენტის რომელიმე ნაწილის მიმართ მოქმედებდეს საპატენტო უფლებები. ისო და იეკი არ არის პასუხისმგებელი რაიმე ან ყველა საპატენტო უფლების იდენტიფიკაციაზე. მოცემული დოკუმენტის შემუშავებისას გამოვლენილი ნებისმიერი დეტალური ინფორმაცია საპატენტო უფლებების შესახებ, წარმოდგენილი იქნება შესავალ ნაწილში ან/და საპატენტოს დეკლარაციების სიაში (იხილეთ, www.iso.org/patents).

წინამდებარე დოკუმენტში გამოყენებული ნებისმიერი სავაჭრო დასახელება მომხმარებელთა ხელშესაწყობად მოწოდებული ინფორმაციაა და არ წარმოადგენს მის რეკლამას.

სტანდარტების ნებაყოფლობითი ხასიათის ასახსნელად და ისოს შესაბამისობის შეფასებასთან დაკავშირებული სპეციალური ცნებებისა და ტერმინოლოგიური შესიტყვებების მნიშვნელობების განსამარტავად, ასევე ისოს მიერ ვაჭრობაში მსოფლიო ორგანიზაციის (ვმო) ტექნიკურ ბარიერების (ტბტ) დებულების დაცვის შესახებ ინფორმაციის გასაცნობად, იხილეთ რესურსის უნიფიცირებული მაჩვენებელი (URL): www.iso.org/iso/foreword.html. იეკში,იხილეთ www.iec.ch./org/understanding-stndards

წინამდებარე დოკუმენტი მოამზადა გაერთიანებულმა ტექნიკურმა კომიტეტმა ისო/იეკ JTC 1-მა, „საინფორმაციო ტექნოლოგიები“, ქვეკომიტეტმა 27, “ინფორმაციის უსაფრთხოების, კიბერუსაფრთხოებისა და საიდუმლოები დაცვის ერთობლივი ტექნიკური კომიტეტი“.

წინამდებარე მესამე რედაქცია აუქმებს და ჩაანაცვლებს მეორე რედაქციას (ისო/იეკ 27001:2013), რომელიც ტექნიკურად გადაიხედა. იგი ასევე მოიცავს ტექნიკურ შესწორებებს: ისო/იეკ 27001:2013/შესწორება 1:2014-სა და ისო/იეკ 27001:2013/შესწორება 2:2015-ს.

ძირითადი ცვლილებები მოიცავს შემდეგს:

- ტექსტი შესაბამისობაში იქნა მოყვანილი მენეჯმენტის სისტემის სტანდარტების ჰარმონიზებულ სტრუქტურასა და ისო/იეკ 27002:2022-სთან.

წინამდებარე დოკუმენტთან დაკავშირებული ნებისმიერი გამოხმაურება ან შეკითხვა უნდა გაეგზავნოს მომხმარებლის ეროვნული სტანდარტიზაციის ორგანოს. ამ ორგანოების სრული სია შეგიძლიათ იხილოთ ბმულზე:-www.is.org/members.html და www.iec.ch/national-committees.

შესავალი

0.1 ზოგადი

წინამდებარე დოკუმენტი მომზადდა ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის ჩამოყალიბების, დანერგვის, შენარჩუნებისა და მუდმივი გაუმჯობესებისთვის საჭირო მოთხოვნების უზრუნველსაყოფად. ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის დანერგვა ორგანიზაციისთვის სტრატეგიული გადაწყვეტილებაა. ორგანიზაციის ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის ჩამოყალიბებასა და დანერგვაზე გავლენას ახდენს ორგანიზაციის საჭიროებები და მიზნები, უსაფრთხოების მოთხოვნები, გამოყენებული საორგანიზაციო პროცესები და ორგანიზაციის სიდიდე და სტრუქტურა. მოსალოდნელია, რომ გავლენის მქონე ყველა ეს ფაქტორი დროთა განმავლობაში შეიცვლება.

ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემა ემსახურება ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის შენარჩუნებას რისკის მართვის პროცესის გამოყენებით, რათა დაინტერესებულმა მხარეებმა უფრო თავდაჯერებულად და ადეკვატურად მართოს რისკები.

მნიშვნელოვანია, რომ ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემა ჩართული იყოს ორგანიზაციის პროცესებსა და მენეჯმენტის მთლიან სტრუქტურაში. წარმოადგენდეს მის ნაწილს, ინფორმაციის უსაფრთხოება გათვალისწინებული უნდა იყოს პროცესების, საინფორმაციო სისტემებისა და კონტროლის დაგეგმვისას. მოსალოდნელია, რომ ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის დანერგვის მასშტაბი განისაზღვროს ორგანიზაციის საჭიროებების შესაბამისად.

წინამდებარე დოკუმენტი შეიძლება გამოიყენებოდეს შიდა და გარე მხარეების მიერ ორგანიზაციის შესაძლებლობის შესაფასებლად, თუ როგორ აკმაყოფილებენ ისინი საკუთარი ორგანიზაციის ინფორმაციის უსაფრთხოების მოთხოვნებს.

წინამდებარე დოკუმენტში მოთხოვნების თანმიმდევრობა არ ასახავს მათ მნიშვნელობას და არ გულისხმობს მათი განხორციელების თანმიმდევრობას. სიის ელემენტები ჩამოთვლილია მხოლოდ საცნობარო მიზნებისთვის.

ისო/იეკ 27000-ში მოცემულია ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემების მიმოხილვა და ლექსიკონი, ასევე მითითებულია ინფორმაციის უსაფრთხოების მენეჯმენტის სისტემის სტანდარტების ჯგუფები (მათ შორის ისო/იეკ 27003[2], ისო/იეკ 27004[3] და ისო/იეკ 27005[4]), შესაბამისი ტერმინებითა და განმარტებებით.

0.2 თავსებადობა მენეჯმენტის სისტემის სხვა სტანდარტებთან

წინამდებარე დოკუმენტში გამოყენებულია მაღალი დონის სტრუქტურა, ქვეპუნქტების იდენტური სათაურები, იდენტური ტექსტი, საერთო ტერმინები და ძირითადი განმარტებები, განსაზღვრულია ისო/იეკ დირექტივების დანართ SL-ის,

ნაწილ 1-ში, ისოს გაერთიანებულ დანართში, შესაბამისად ის თავსებადია მენეჯმენტის სისტემის სხვა სტანდარტებთან, რომლებმაც მიიღეს დანართი SL.

დანართი SL-ში განსაზღვრული ეს საერთო მიდგომა სასარგებლო იქნება იმ ორგანიზაციებისთვის, რომლებიც უპირატესობას ანიჭებენ მენეჯმენტის ერთიან სისტემას, და აკმაყოფილებენ მენეჯმენტის სისტემის ორი ან მეტი სტანდარტის მოთხოვნებს.