საქართველოს სტანდარტი

სსკ 01.040.35; 03.100.70; 35.030

საინფორმაციო ტექნოლოგია - უსაფრთხოების მეთოდები - ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები - ზოგადი მიმოხილვა და ტერმინოლოგია

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 2022 წლის 15 სეტემბრის №64 განკარგულებით სტანდარტიზაციის ტექნიკური კომიტეტის, ტკ 2-ის, „მენეჯმენტი და შესაბამისობის შეფასება“ გადაწყვეტილების საფუძველზე.

3 წინამდებარე სტანდარტი წარმოადგენს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ისო-ს) და საერთაშორისო ელექტროტექნიკური კომისის (იეკ-ის) სტანდარტის ისო/იეკ 27000:2018 „საინფორმაციო ტექნოლოგია - უსაფრთხოების მეთოდები - ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები - ზოგადი მიმოხილვა და ტერმინოლოგია“ იდენტურ თარგმანს (IDT).

4 პირველად

5 რეგისტრირებულია: სსიპ - საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს საქართველოს სტანდარტების რეესტრში 2022 წლის 15 სექტემბერი №268-1.1-00452

სარჩევი

წინასიტყვაობა V
შესავალი VII
1 გამოყენების სფერო 1
2 ნორმატიული მითითებები 1
3 ტერმინები და განმარტებები 1
4 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები 15
4.1 ზოგადი 15
4.2 რას გულისხმობს ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები (ISMS)? 16
4.2.1 ზოგადი მიმოხილვა და პრინციპები 16
4.2.2 ინფორმაცია 17
4.2.3 ინფორმაციული უსაფრთხოება 17
4.2.4 მენეჯმენტი 18
4.2.5 მენეჯმენტის სისტემა 18
4.3 პროცესული მიდგომა 19
4.4 რატომ არის მნიშვნელოვანი ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები (ISMS)? 19
4.5 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) შემუშავება, მონიტორინგი, უზრუნველყოფა და გაუმჯობესება 20
4.5.1 ზოგადი მიმოხილვა 20
4.5.2 ინფორმაციული უსაფრთხოების მოთხოვნების განსაზღვრა 21
4.5.3 ინფორმაციული უსაფრთხოების რისკების შეფასება 21
4.5.4 ინფორმაციული უსაფრთხოების რისკების დამუშავება 22
4.5.5 მართვის საშუალებების შერჩევა და დანერგვა 22
4.5.6 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) ეფექტურობის მონიტორინგი, უზრუნველყოფა და გაუმჯობესება 24
4.5.7 მუდმივი გაუმჯობესება 24
4.6 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) წარმატებების კრიზისული ფაქტორები 25
4.7 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების სტანდარტების ოჯახის უპირატესობები 25
5 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) სტანდარტების ოჯახი 26
5.1 ზოგადი ინფორმაცია 26
5.2 სტანდარტი, რომელიც აღწერს ზოგად მიმოხილვასა და ტერმინოლოგიას: ისო/იეკ 27000 (წინამდებარე დოკუმენტი) 27

5.3 მოთხოვნების განმსაზღვრელი სტანდარტები 28
5.3.1 ისო/იეკ 27001 28
5.3.2 ისო/იეკ 27006 28
5.3.3 ისო/იეკ 27009 29
5.4 სტანდარტები, რომლებიც აღწერს ზოგად სახელმძღვანელო მითითებებს : 29
5.4.1 ისო/იეკ 27002 29
5.4.2 ისო/იეკ 27003 30
5.4.3 ისო/იეკ 27004 30
5.4.4 ისო/იეკ 27005 30
5.4.5 ისო/იეკ 27007 31
5.4.6 ისო/იეკ ტრ 27008 31
5.4.7 ისო/იეკ 27013 31
5.4.8 ისო/იეკ 27014 32
5.4.9 ისო/იეკ ტრ 27016 32
5.4.10 ისო/იეკ 27021 33
5.5 სტანდარტები, რომლებიც აღწერს დარგობრივ სახელმძღვანელო მითითებებს: 33
5.5.1 ისო/იეკ 27010 33
5.5.2 ისო/იეკ 27011 34
5.5.3 ისო/იეკ 27017 34
5.5.4 ისო/იეკ 27018 35
5.5.5 ისო/იეკ 27019 35
5.5.6 ისო 27799 36

ბიბლიოგრაფია 38

წინასიტყვაობა

ისო (სტანდარტიზაციის საერთაშორისო ორგანიზაცია) ეროვნული სტანდარტების ორგანოების (ისო-ს წევრი კომიტეტების) მსოფლიო ფედერაციაა. საერთაშორისო სტანდარტები, ჩვეულებრივ, მზადდება ისო-ს ტექნიკური კომიტეტების მიერ. თითოეულ წევრ კომიტეტს, აქვს უფლება მისთვის საინტერესო საკითხთან დაკავშირებით შექმნილ ტექნიკურ კომიტეტში გაერთიანდეს. ამ სამუშაოში მონაწილეობენ ასევე ისოს-თან დაკავშირებული სამთავრობო და არასამთავრობო საერთაშორისო ორგანიზაციები. ისო მჭიდროდ თანამშრომლობს საერთაშორისო ელექტროტექნიკურ კომისიასთან (იეკ-თან) ელექტროტექნიკური სტანდარტიზაციის ყველა საკითხზე.

წინამდებარე დოკუმენტის შესამუშავებლად და მისი შემდგომი გამოყენებისთვის განკუთვნილი მეთოდები აღწერილია ისო/იეკის დირექტივების 1-ელ ნაწილში, კერძოდ, უნდა აღინიშნოს დამტკიცების სხვადასხვა კრიტერიუმი ისო-ს სხვადასხვა ტიპის დოკუმენტისთვის. წინამდებარე დოკუმენტი შედგენილია ისო/იეკ-ის დირექტივების მე-2 ნაწილის სარედაქციო წესების შესაბამისად (იხილეთ. www.iso.org/directives).

ყურადღებას იქცევს ალბათობა იმისა, რომ საერთაშორისო სტანდარტის ზოგიერთ ნაწილს შესაძლებელია შეეხოს საპატენტო უფლებები. ისო არ იღებს პასუხისმგებლობას რომელიმე ან ყველა მსგავსი საპატენტო უფლების დადგენაზე. დოკუმენტის შემუშავებისას გამოვლენილი დეტალური ინფორმაცია ნებისმიერი საპატენტო უფლების შესახებ წარმოდგენილი იქნება შესავალში და/ან ისო-ს საპატენტო დეკლარაციების სიაში(იხილეთ www.iso.org/patents).

წინამდებარე დოკუმენტში გამოყენებული ნებისმიერი სავაჭრო დასახელება მომხმარებლების ხელშესაწყობად წარმოდგენილი ინფორმაციაა და არ არის სასაქონლო ნიშნის მხარდამჭერი.

. სტანდარტების ნებაყოფლობითი ბუნების ასახსნელად და ისო-ს შესაბამისობის შეფასებასთან დაკავშირებული სპეციალური ტერმინებისა და ტერმინოლოგიური შესიტყვებების მნიშვნელობების განსამარტავად, ასევე ისო-ს მიერ ვაჭრობაში მსოფლიო ორგანიზაციის (ვმო) ტექნიკური ბარიერების (ტბტ) დებულებების დაცვის შესახებ ინფორმაციის გასაცნობად იხილეთ რესურსის უნიფიცირებული მაჩვენებელი (URL): www.iso.org/iso/foreword.html.

წინამდებარე დოკუმენტი მომზადდა ტექნიკური კომიტეტის, ისო/იეკ ეტკ 1-ის, (ერთობლივი ტექნიკური კომიტეტი) საინფორმაციო ტექნოლოგიები, ქკ 27, საინფორმაციო ტექნოლოგიების (IT) უსაფრთხოების მეთოდები, მიერ.

წინამდებარე მეხუთე გამოცემა აუქმებს და ცვლის მეოთხე გამოცემას (ისო/იეკ 27000:2016), რომელიც ტექნიკურად გადაიხედა. ძირითადი ცვლილებები წინა გამოცემასთან შედარებით არის შემდეგი:

- ხელახლა ჩამოყალიბდა შესავალი;
- ამოღებულია ზოგიერთი ტერმინი და განმარტება;
- მე-3 თავი შეესაბამა უსაფრთხოების მომსახურების მენეჯმენტისათვის მაღალი დონის სტრუქტურას;
- განახლდა მე-5 თავი შესაბამის სტანდარტებში ცვლილებების ასახვისათვის;
- A და B დანართები ამოღებულია.