
მზად ხართ ინფორმაციული
უსაფრთხოების
განახლებულ კანონთან
შესაბამისობისთვის?
The better the question.
The better the answer.
The better the world works.
EY
Building a better
working world

ცვლილებები ინფორმაციული უსაფრთხოების კანონში

2012 წლიდან ქვეყანაში მოქმედებს ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონი, რომელიც ადგენს ინფორმაციული უსაფრთხოების ძირითად სტანდარტებს.

კანონის მიზანია ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

600%

გაზრდილია კიბერდანაშაულების გლობალური სტატისტიკა მიმდინარე კოვიდპანდემიის ფონზე

2022 წლის პირველი იანვრიდან ძალაში შევიდა მნიშვნელოვანი საკანონმდებლო ცვლილებები:

- გაიზარდა სუბიექტთა წრე, რომლებზეც ვრცელდება კანონი და მოხდა მათი კატეგორიზაცია
- კატეგორიების მიხედვით შეიცვალა მაკოორდინირებელი და ზედამხედველი უწყებები
- კანონის მოთხოვნების შეუსრულებლობაზე განისაზღვრა ადმინისტრაციულ-სამართლებრივი სანქციები.

ვისზე ვრცელდება კანონის მოქმედება?

კანონის მოქმედება ვრცელდება საქართველოს მთავრობის დადგენილებით განსაზღვრულ კრიტიკული ინფორმაციული სისტემის სუბიექტებზე (შემდგომში სუბიექტი).

კრიტიკული ინფორმაციული სისტემის სუბიექტი წარმოადგენს ორგანოს/დაწესებულებას, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.

ახალი ცვლილებით კრიტიკული ინფორმაციული სისტემის სუბიექტი იყოფა სამ კატეგორიად:

კატეგორია	დაწესებულება		საზედამხედველო ორგანო
პირველი კატეგორია	სახელმწიფო ორგანოები / დაწესებულებები		სსიპ ოპერატიულ-ტექნიკური სააგენტო
მეორე კატეგორია	ელექტრონული კომუნიკაციების კომპანიები		სსიპ ოპერატიულ-ტექნიკური სააგენტო
მესამე კატეგორია	კერძო სამართლის იურიდიული პირები	კომერციული ბანკები	სსიპ ციფრული მმართველობის სააგენტო საქართველოს ეროვნული ბანკი
		სადაზღვევო და სატრანსპორტო ორგანიზაციები, ენერგოკომპანიები და სხვა	სსიპ ციფრული მმართველობის სააგენტო

* სუბიექტების სრული სია შეგიძლიათ იხილოთ ბმულზე

რა არის კანონის ძირითადი მოთხოვნები?

ინფ. უსაფრთხოების მართვის სისტემის დანერგვა

სუბიექტი ვალდებულია, კანონმდებლობით განსაზღვრულ ვადებში შეიმუშაოს და დანერგოს ინფ. უსაფრთხოების მართვის სისტემა

ინფ. უსაფრთხოების აუდიტი

სუბიექტი ვალდებულია ჩაატაროს ინფორმაციული უსაფრთხოების პირველადი და პერიოდული აუდიტი მინიმალურ სტანდარტებთან შესაბამისობაზე

შეღწევადობის ტესტირება

სუბიექტი ვალდებულია ჩაატაროს ინფორმაციულ სისტემაში შეღწევადობის ტესტი

ინფ. უსაფრთხოების მენეჯერი

სუბიექტი ვალდებულია განსაზღვროს ორგანიზაციაში ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებაზე პასუხისმგებელი პირი

რა არის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები?

სუბიექტი ვალდებულია მიიღოს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები და განსაზღვროს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც აკმაყოფილებს ზედამხედველი ორგანოს მიერ დადგენილ ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (ISO/IEC 27001).

პირველი/მეორე კატეგორიის სუბიექტი ვალდებულია, კრიტიკული ინფორმაციული სისტემის სუბიექტად განსაზღვრიდან **2 წლის ვადაში** დანერგოს ინფორმაციული უსაფრთხოების მართვის სისტემა. **მესამე კატეგორიის სუბიექტი** ვალდებულია, მთავრობის დადგენილებით დამტკიცებულ ნუსხაში შეყვანის მომენტიდან **3 კალენდარული წლის ვადაში** დანერგოს მართვის სისტემა მარეგულირებლის მიერ განსაზღვრული შემდეგი მოთხოვნების შესაბამისად:

პირველი წელი: დაგეგმვა	მეორე წელი: დანერგვა	მესამე წელი: მონიტორინგი და გაუმჯობესება
▸ ხელმძღვანელობის მხარდაჭერა ▸ ორგანიზაციული მოწყობა ▸ იუმს-ის გავრცელების სფეროს განსაზღვრა ▸ იუმს-ის პოლიტიკის შემუშავება და დამტკიცება ▸ აქტივების მართვა და რისკების შეფასება ▸ კონტროლის მექანიზმების გამოყენებადობის განაცხადის მომზადება ▸ ინფ. უსაფრთხოების ამოცანები და მათი შესრულების გეგმები ▸ იუმს-ის დოკუმენტაციის მართვა	▸ რისკების მოპყრობის გეგმის დანერგვა ▸ ორგანიზაციაში კონტროლის მექანიზმების დანერგვა ▸ კონტროლის მექანიზმების ეფექტიანობის საზომების განსაზღვრა ▸ ტრენინგები, ცნობიერების ამაღლება და კომპეტენციები	▸ იუმს-ის მონიტორინგისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა ▸ ორგანიზაციაში იუმს-ის შიდა აუდიტის ჩატარება ▸ ხელმძღვანელობის მიერ იუმს-ის განხილვა ▸ შეუსაბამობების მაკორექტირებელი ქმედებები ▸ იუმს-ის გაუმჯობესება და კომუნიკაცია

ადმინისტრაციულ-სამართლებრივი სანქციები

ინფორმაციული უსაფრთხოების კანონმდებლობით დადგენილი მოთხოვნების შეუსრულებლობაზე განისაზღვრა ადმინისტრაციული სანქციები. სხვადასხვა კატეგორიის ადმინისტრაციულ სამართალდარღვევისთვის კანონით გათვალისწინებულია **5,000-დან 20,000 ლარამდე** ჯარიმა (მესამე კატეგორიის სუბიექტებისთვის კი **საზედამხედველო კაპიტალის** 0.01%, 0.05% **ან** 0.1%, **მინიმუმ** 20 000 **ლარი**), მათ შორის ინფორმაციული უსაფრთხოების აუდიტის ან შეღწევადობის ტესტის ჩატარების ვალდებულების შეუსრულებლობაზე

როგორ შეგვიძლია თქვენი დახმარება?

იუაის ჰყავს გამოცდილი კონსულტანტებით დაკომპლექტებული გუნდი, რომელიც უკვე წლებია ეხმარება ორგანიზაციებს სხვადასხვა ინდუსტრიიდან დაიცვან საკუთარი ინფორმაციული აქტივები, გაუმჯობესონ ტექნოლოგიური შესაძლებლობები, უზრუნველყონ შესაბამისობა ადგილობრივ და საერთაშორისო რეგულაციებთან და განავითარონ თავიანთი ბიზნესი ეფექტური ინფორმაციული უსაფრთხოებით. ჩვენ შევიმუშავეთ 6 ძირითადი მიმართულება, რომლებიც დაგეხმარებათ ახალი მარეგულირებელი მოთხოვნების დაკმაყოფილებასა და უსაფრთხოების მაღალი სტანდარტის უზრუნველყოფაში.

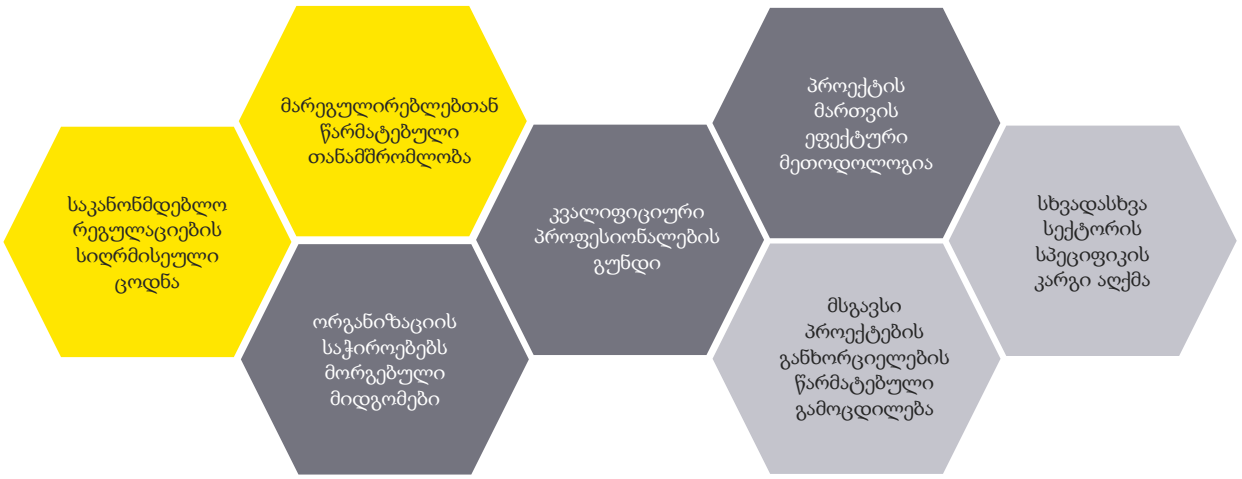
ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა	იუმს-ის პროგრამის შემუშავება და იმპლემენტაცია, მათ შორის კრიტიკული ინფორმაციის გამოვლენა, კლასიფიკაცია და მართვა	▸ არსებული მდგომარეობის შეფასება (ე. წ. Gap analysis) ▸ ორგანიზაციის საჭიროებებზე მორგებული იუმს-ის პროგრამის შემუშავება ▸ იუმს-ის პროგრამის დანერგვა
ინფორმაციული უსაფრთხოების სისტემების იმპლემენტაცია	ინტეგრატორებთან კონსორციუმში ორგანიზაციის მხარდაჭერა ინფორმაციული უსაფრთხოების სისტემების (მაგ., DLP, SIEM, IPS) დანერგვის პროცესში	▸ ორგანიზაციის საჭიროების შესწავლა და სატენდერო დოკუმენტაციის (მაგ., ტექნიკური დავალება, საკვალიფიკაციო მოთხოვნები და ა. შ.) შემუშავება ▸ მომწოდებლებთან კონსორციუმში სისტემების დანერგვა და ორგანიზაციის სპეციფიკაციებზე მორგება
ინფორმაციული უსაფრთხოების აუდიტი / შეფასება	მართვის სისტემის ზედამხედველი ორგანოს მიერ დადგენილ მინიმალურ მოთხოვნებთან შესაბამისობა	▸ ინფორმაციული უსაფრთხოების აუდიტი / შეფასება ▸ საკონსულტაციო მომსახურება - აუდიტის შედეგად გამოვლენილ შეუსაბამობებზე კანონით გათვალისწინებული საპასუხო სამოქმედო გეგმისა და გზამკვლევის მომზადებაზე
ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროგრამის შემუშავება	ინციდენტებზე რეაგირების ჩარჩოს, მეთოდოლოგიისა და პროცედურების შემუშავება	▸ ინციდენტებზე რეაგირების ჩარჩოს შემუშავება ▸ ინციდენტის მართვის სასიცოცხლო ციკლისა და რეაგირების მეთოდოლოგიის განსაზღვრა ▸ ინციდენტის გამოვლენის, შეკავების, აღმოფხვრისა და აღდგენის პროცედურები და ინსტრუქციები ▸ რეაგირების გეგმების ტესტირება და რეკომენდაციების შემუშავება ▸ გამოყენებული სისტემების / საშუალებების ტესტირება
შეღწევადობის ტესტი / Red Teaming	მავნე აქტორების მიერ რეალურ ცხოვრებაში გამოყენებული ტექნიკებისა და მეთოდების სიმულაცია	▸ შეტევების სიმულაციის გზით ორგანიზაციის დაცვის მექანიზმების სისუსტეების გამოვლენა, მათი ექსპლუატაციის შესაძლებლობის შეფასება და შესაბამისი რეკომენდაციების შემუშავება ▸ საკონსულტაციო მომსახურება - შეღწევადობის ტესტის შედეგად გამოვლენილ მოწყვლადობაზე კანონით გათვალისწინებული საპასუხო სამოქმედო გეგმისა და გზამკვლევის მომზადება
ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლება	ორგანიზაციის თანამშრომლებისთვის უსაფრთხოების ძირითად საფრთხეებსა და შესაბამის დაცვის მექანიზმებზე ცნობიერების ამაღლება	▸ ინფორმაციულ უსაფრთხოებაზე ცნობიერების ამაღლების ტრენინგი სხვადასხვა სამიზნე ჯგუფისთვის, მაგალითად: C-Level, პრივილეგირებული მომხმარებლები, სტანდარტული მომხმარებლები, ფიზიკური უსაფრთხოების სპეციალისტები და ა. შ. ▸ სოციალური ინჟინერიის ტესტები (მაგ., Self-Phishing) ▸ ცნობიერების ამაღლების ონლაინ პლატფორმის იმპლემენტაცია და მხარდაჭერა

საქართველოში განხორციელებული პროექტები

იუაი საქართველოს გუნდმა წარმატებით განახორციელა არაერთი პროექტი ინფორმაციული უსაფრთხოებისა და ტექნოლოგიების სფეროში. ძირითადი პროექტები მოცემულია ცხრილში:

#	ორგანიზაციის დასახელება	პროექტის დასახელება
1	ელექტროენერგიის გადამცემი სისტემის ოპერატორი	ინფორმაციული უსაფრთხოების მართვის სისტემის ISO/IEC 27001 უსაფრთხოების სტანდარტის შესაბამისად ორგანიზება და დანერგვა
2	წამყვანი სამი ქართული ბანკი	ინფორმაციული უსაფრთხოების მართვის სისტემის ISO/IEC 27001 უსაფრთხოების სტანდარტის მიმართ შიდა აუდიტი
3	წამყვანი სამი ქართული ბანკი	ინფორმაციული უსაფრთხოების მართვის სისტემის ISO/IEC 27001 უსაფრთხოების სტანდარტის მიმართ დამოუკიდებელი შეფასება
4	წამყვანი სამი ქართული ბანკი	შიდა IT აუდიტის ფუნქციის ქოსორსინგის ფარგლებში ჩატარებული 7 პროექტი, მათ შორის, კიბერუსაფრთხოების, IT და მესამე მხარეების რისკების მართვის აუდიტები.
5	წამყვანი ათი ქართული ბანკი	ინფორმაციული უსაფრთხოების პროცესებისა და კონტროლების საქართველოს ეროვნული ბანკის კიბერუსაფრთხოების მართვის ჩარჩოს მიმართ აუდიტი
6	წამყვანი ათი ქართული ბანკი	სვიფტის მომხმარებელთა უსაფრთხოების პროგრამის მიმართ აუდიტი
7	წამყვანი ათი ქართული ბანკი	PSD2 Open API შეღწევადობის ტესტირება
8	ელექტროენერგიის დისტრიბუტორი ორგანიზაცია	IT და ინფორმაციული უსაფრთხოების პროცესებისა და პოლიტიკების შემუშავება
9	სსიპ „სახელმწიფო სერვისების განვითარების სააგენტო“	სანდო და კვალიფიციური სანდო მომსახურების (მაგ., ელ. ხელმოწერა და შტამპი) European Telecommunications Standards Institute (ETSI) სტანდარტის მიმართ აუდიტი

იუაისთან თანამშრომლობის უპირატესობები



იუაის შესახებ

იუაი არის მსოფლიო ლიდერი აუდიტორული, საგადასახადო, იურიდიული და საკონსულტაციო მომსახურების სფეროში. ჩვენი საქმის სიღრმისეული ცოდნითა და მომსახურების მაღალი ხარისხით ხელს ვუწყობთ კაპიტალის ბაზრებისა და ეკონომიკის მიმართ ნდობის გაღრმავებას. ამასთანავე ვაყალიბებთ გამორჩეულ ლიდერებს, რომელთა ხელმძღვანელობითაც ყოველთვის ვასრულებთ ყველა დაინტერესებული მხარის მიმართ აღებულ ვალდებულებებს და ამით უმნიშვნელოვანესი წვლილი შეგვაქვს ჩვენი თანამშრომლებისთვის, კლიენტებისთვის და ფართო საზოგადოებისთვის საქმიანი გარემოს გაუმჯობესებაში.

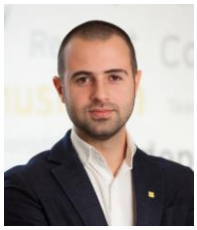
კომპანიის სახელწოდება იუაი აღნიშნავს ,,ერნსტ ენდ იანგ გლობალ ლიმიტედის'' წევრი ფირმების გლობალურ გაერთიანებას ან მის ერთ ან ერთზე მეტ წევრ ფირმას, რომელთაგან თითოეული დამოუკიდებელი იურიდიული ერთეულია. თავად ,,ერნსტ ენდ იანგ გლობალ ლიმიტედ'', გაერთიანებულ სამეფოში დაფუძნებული გარანტიით შეზღუდული კომპანია, კლიენტებს მომსახურებას არ უწევს.

იუაის საკონსულტაციო მომსახურების შესახებ

იუაის საკონსულტაციო გუნდს მიგვაჩნია, რომ სამყაროში უკეთესი სამუშაო გარემოს შექმნა გულისხმობს კლიენტების დახმარებას მსხვილი და კომპლექსური ინდუსტრიული გამოწვევების გადაჭრაში და იმ შესაძლებლობების ეფექტურ გამოყენებაში, რომლებიც დაეხმარება ბიზნესს გაიზარდოს, გახდეს ოპტიმალური და იყოს დაცული.

გლობალური აზროვნება, მრავალფეროვნება და თანამშრომლობითი კულტურა შთააგონებს იუაის კონსულტანტებს დასვან სწორი კითხვები, ეძიონ პასუხები და უზრუნველყონ გრძელვადიანი შედეგები.

საკონტაქტო პირი



გიორგი ცინცქილაძე
ბიზნესსაკონსულტაციო დეპარტამენტის ხელმძღვანელი, ტექნოლოგიური რისკების ჯგუფი
+995 32 215 88 11
Giorgi.Tsintskiladze@ge.ey.com