ტექნიკური დავალება

სახელმწიფო აუდიტის სამსახურის ინფორმაციული უსაფრთხოების საერთაშორისო სტანდარტთან (ISO/IEC 27001: 2013) შესაბამისობის შეფასება

სახელმწიფო აუდიტის სამსახურს ესაჭიროება აუდიტის მომსახურება, რათა შეფასდეს კომპანიის მზაობა ISO/IEC 27001:2013-ის დანერგვისთვის და შემდგომი სერტიფიცირებისთვის, იდენტიფიცირებული იყოს ხარვეზები და პოტენციური რისკები. შემუშავდეს მათი აღმოფხვრის სტრატეგია.

პროცესი უნდა მოიცავდეს:

1. **ინტერვიუები კომპანიის სხვადასხვა სტრუქტურულ ერთეულთან:**

   ა) მენეჯმენტთან

   ბ) IT სამსახურთან

   გ) დეველოპერების ხელმძღვანელთან

   დ) რისკების მართვაზე პასუხისმგებელ პირთან

   ე) HR თან

2. **კომპანიაში არსებული პოლიტიკის/პროცედურების გაცნობა:**

   ა) IT აქტივების ინვენტარი

   ბ) რისკების შეფასებისა და მათთან მოპყრობის პროცედურები

   გ) ინფორმაციული უსაფრთხოების პოლიტიკები

   დ) ცვლილებების, ინციდენტების, მართვა

   ე) არსებული კონტროლის მექანიზმების ეფექტურობის შეფასება

ამ და სხვა პროცესებისთვის გაწერილი პოლიტიკების სამსახურში არსებულ რეალურ სურათთან შედარება და შეუსაბამობების იდენტიფიცირება.

შეფასებული უნდა იქნას ინფორმაციული უსაფრთხოების მართვის სისტემის შემდეგი კომპონენტები:

1. პოლიტიკები და პროცედურები;

2. რისკების მართვის პროცესი

3. ცნობიერების ამაღლების პროცესი

4. ტექნიკური კონტროლის მექანიზმების ეფექტურობა

5. ადამიანური რესურსების უსაფრთხოების მართვის პროცესი

6. წვდომის კონტროლის პროცესი

7. ინფორმაციული აქტივების მართვის პროცესი

8. ფიზიკური უსაფრთხოება

9. IT ოპერაციების უსაფრთხოება

10. მესამე მხარეებთან უსაფრთხოების მართვის პროცესი

11. ინციდენტების მართვის პროცესი

12. ბიზნეს უწყვეტობის მართვის პროცესი

13. შესაბამისობის მართვის პროცესი

ინფორმაციული უსაფრთხოების მართვის სისტემის მასშტაბი (Scope):

1. ბიზნეს პროცესების რაოდენობა - 3
2. თანამშრომლების რაოდენობა - 300
3. ფიზიკური ლოკაცია - 3

შეფასების შემდგომ მომწოდებელმა უნდა უზრუნველყოს სამსახურისთვის შემდეგი დოკუმენტების მოწოდება როგორც ციფრული, ისე მატერიალური სახით:

1. ISO/IEC 27001:2013 სტანდარტთან შესაბამისობის ანგარიში (Gap Assessment Report)
2. ISO/IEC 27001:2013 სტანდარტის დანერგვის სამოქმედო გეგმა (Action Plan)

სერვისის მოწოდების ვადა: ხელშეკრულების გაფორმებიდან არაუმეტეს 14 კალენდარული დღის განმავლობაში;

მომწოდებელი უნდა აკმაყოფილებდეს შემდეგ პირობებს:

1. განხორციელებული უნდა ჰქონდეს სულ მცირე ერთი მსგავსი პროექტი
2. დასაქმებული უნდა ჰყავდეს სერტიფიცირებული გუნდის წევრები:

a. ISO/IEC 27001:2013 Lead Auditor.

b. Certified Information Systems Auditor - CISA

შენიშვნა:

1. წარმოდგენილ ტექნიკური დავალებაში პრეტენდენტმა ზუსტად უნდა განსაზღვროს გასაწევი (შემოთავაზებული) მომსახურება.
2. დოკუმენტი დადასტურებული უნდა იყოს პრეტენდენტის კვალიფიციური ელექტრონული ხელმოწერით ან/და კვალიფიციური ელექტრონული შტამპით