სს „ხალიკ ბანკი საქართველოს“ ინფორმაციული უსაფრთხოების პოლიტიკა

თბილისი

2025წ.

სარჩევი

1. ზოგადი დებულება

სს „ხალიკ ბანკი საქართველოს“ (შემდგომში - ბანკი) ინფორმაციული უსაფრთხოების პოლიტიკა (შემდგომში - „პოლიტიკა“) განსაზღვრავს ინფორმაციის დაცვის ძირითად პრინციპებს და მოთხოვნებს, აგრეთვე, ბანკის თანამშრომელთა და სხვა მომხმარებელთა მიერ, ინფორმაციის, ინფორმაციული ტექნოლოგიებისა და ინფორმაციული სისტემების მოხმარების წესებს. პოლიტიკის მარეგულირებელ და სამართლებრივ საფუძველს წარმოადგენს საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, საქართველოს ეროვნული ბანკის რეგულაცია კიბერუსაფრთხოების მართვის ჩარჩოს შესახებ და კანონი პერსონალურ მონაცემთა დაცვის შესახებ. გარდა ამისა, გათვალისწინებულია ინფორმაციული უსაფრთხოების მართვის სისტემის საერთაშორისო სტანდარტების მოთხოვნები.

2. ტერმინთა განმარტება

ინფორმაციული უსაფრთხოება - საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

ინფორმაციული აქტივი - ყველა სახის ინფორმაცია და ცოდნა, მათ შორის ინფორმაციის შენახვის, დამუშავების, გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ, რომლებიც ღირებულია ბანკისთვის;

კონტროლის მექანიზმი - ნებისმიერი ქმედება, მოწყობილობა, პროცედურა ან სხვა ღონისძიება, რომელიც გამოიყენება რისკის შესამცირებლად და ინფორმაციის აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის (CIA) დასაცავად. ეს არის საფრთხეების და დაუცველობის მართვის გზა უსაფრთხოების ინციდენტების თავიდან ასაცილებლად ან მათი ზემოქმედების მინიმუმამდე შესამცირებლად.

ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს) - ბანკის შიდა ორგანიზაციული მართვის სისტემის განუყოფელი ნაწილი, რომელიც დაფუძნებულია რისკების მართვის პრინციპებზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების მოთხოვნების დანერგვა, ფუნქციონირება, მონიტორინგი, შეფასება, მხარდაჭერა და გაუმჯობესება.

3. პოლიტიკის მიზანი

წინამდებარე პოლიტიკის მიზანია შიდა და გარე საფრთხეების მიმართ ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების განსაზღვრა. პოლიტიკა მიზნად ისახავს ბანკში არსებული ინფორმაციის, საქართველოს კანონმდებლობით და საქართველოს ეროვნული ბანკის მიერ დაკისრებული ფუნქციებისა და ბანკის რეპუტაციის დასაცავად კონტროლის მექანიზმების შექმნას და მისი მეშვეობით ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფას. ამასთან, პოლიტიკის მიზანია:

- ინფორმაციისა და მასთან დაკავშირებული ინფრასტრუქტურული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა და შენარჩუნება;
- უსაფრთხოების დარღვევის ან კომპრომეტირების რისკის მართვა;
- უსაფრთხო და სტაბილური საინფორმაციო ტექნოლოგიების გარემოს უზრუნველყოფა;
- ინფორმაციული აქტივების არასწორად გამოყენების, დაკარგვის ან/და არაავტორიზებული გამჟღავნების შემთხვევების იდენტიფიცირება და რეაგირება;
- სისტემების მონიტორინგზე კომპრომეტირების შესაძლო ნიშნების აღმოჩენა;
- უზრუნველყოს ბანკის ინფორმაციული უსაფრთხოების მართვის პროცესის მონიტორინგი, ანალიზი და მუდმივი გაუმჯობესება;
- ინფორმაციული უსაფრთხოების შესახებ ცნობიერების ამაღლება და მისი გაუმჯობესება.

4. პოლიტიკის გავრცელების სფერო

პოლიტიკა ვრცელდება ბანკის საკუთრებაში არსებულ ყველა ტიპის ინფორმაციულ აქტივზე, განურჩევლად მათი ფორმისა თუ ფორმატისა. ეს მოიცავს, როგორც ელექტრონულ, ისე ფიზიკურ აქტივებს, რომლებიც იქმნება ან/და გამოიყენება ბანკის ბიზნეს საქმიანობის მხარდასაჭერად. პოლიტიკით განსაზღვრული მოთხოვნების დაცვა სავალდებულოა ბანკის ყველა თანამშრომლისთვის, სტაჟიორისთვის, კონტრაქტორისა და ნებისმიერი მესამე მხარისთვის, რომელთაც გააჩნიათ რაიმე სახის წვდომა ბანკის ინფორმაციულ აქტივებზე. ისინი ვალდებულნი არიან სრულად შეასრულონ ინფორმაციული უსაფრთხოების წესები და სტანდარტები, რათა უზრუნველყოფილი იყოს ბანკის მონაცემების უსაფრთხოება.

5. ლიდერობა

ბანკის უმაღლესი რგოლის ხელმძღვანელობა იღებს პასუხისმგებლობას იუმს-ის მართვის პროცესზე, ახდენს ლიდერობისა და ნაკისრი ვალდებულებების დემონსტრირებას და ორგანიზაციული ფუნქციების განსაზღვრით აყალიბებს შესაბამის მიდგომებს, რაც გამოიხატება შემდეგში:

- ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების მიზნების ჩამოყალიბება და ბანკის სტრატეგიულ მიზნებთან შესაბამისობის უზრუნველყოფა;
- იუმს-ის მოთხოვნების ბანკის პროცესებში ინტეგრირების უზრუნველყოფა;
- იუმს-ის მართვისთვის საჭირო რესურსების ხელმისაწვდომობის უზრუნველყოფა;
- ინფორმაციული უსაფრთხოების ეფექტიანი მართვისა და იუმს-ის მოთხოვნებთან შესაბამისობის მნიშვნელობის კომუნიკაციის უზრუნველყოფა;
- იუმს-ის ფარგლებში დასახული მიზნების დადგენა და მიღწევა;
- იუმს-ის მუდმივი გაუმჯობესების ხელშეწყობის უზრუნველყოფა;
- უსაფრთხოების ინციდენტების სათანადოდ მართვის უზრუნველყოფა და მათგან მიღებული გამოცდილების გამოყენება იუმს-ის გასაუმჯობესებლად.

ამასთან, ბანკში ინფორმაციული უსაფრთხოების მხარდაჭერას უზრუნველყოფს ბანკის ყველა თანამშრომელი.
გარდა ამისა, უმაღლესი რგოლის ხელმძღვანელობა რეგულარულად ატარებს იუმს-ის წარმადობის სისტემატურ გადახედვას, რათა უზრუნველყოს ხარისხის მიზნების შესრულება და შესაბამისი შეუსაბამობების იდენტიფიცირება აუდიტისა და მმართველობითი პროცესების საშუალებით.

6. ინფორმაციული უსაფრთხოების სამუშაო ჯგუფი

ბანკში შექმნილია ინფორმაციული უსაფრთხოების სამუშაო ჯგუფი, რომლის მთავარი მიზანია ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს-ის) ეფექტიანი ფუნქციონირების, შესაბამისობისა და ადეკვატურობის უზრუნველყოფა.

ინფორმაციული უსაფრთხოების სამუშაო ჯგუფის მიზანი, ამოცანები, ფუნქციები, ჯგუფის შემადგენლობა, რეგლამენტი და ორგანიზაციულ-ტექნიკური მხარდაჭერის დეტალები სრულად არის ასახული - „ინფორმაციული უსაფრთხოების სამუშაო ჯგუფის დებულებაში“.

7. აქტივების მართვა

ბანკი უზრუნველყოფს ინფორმაციული აქტივების ეფექტურ იდენტიფიკაციასა და კლასიფიკაციას, რათა მათ სათანადო დაცვა მოხდეს მთელი სასიცოცხლო ციკლის განმავლობაში. ამ პროცესის ფარგლებში:

- ხდება ყველა ინფორმაციული აქტივის გამოვლენა და მათი კლასიფიცირება მისი მგრძნობელობისა და კრიტიკულობის მიხედვით;
- მკაფიოდ არის განსაზღვრული აქტივების მოპყრობის, შეცვლისა და განადგურების წესები მათი კლასიფიკაციის შესაბამისად;
- ყოველი იდენტიფიცირებული აქტივისთვის განსაზღვრულია პასუხისმგებელი პირი (მფლობელი), რომელიც უზრუნველყოფს მის სათანადო მართვასა და დაცვას.

ინფორმაციული აქტივების იდენტიფიცირებისა და კლასიფიკაციის დეტალური წესები განისაზღვრება ბანკის შიდა დოკუმენტებით.

8. რისკების მართვა

ბანკის ინფორმაციული უსაფრთხოების მართვის სისტემა დაფუძნებულია ინფორმაციული უსაფრთხოების რისკების მართვის უწყვეტ პროცესზე, რომელიც რეგულირდება „ინფორმაციული ტექნოლოგიებისა და ინფორმაციული უსაფრთხოების რისკების მართვის პოლიტიკით“. ამ პროცესის ფარგლებში ბანკი ახორციელებს შემდეგ მნიშვნელოვან აქტივობებს:

- შიდა და გარე საფრთხეების იდენტიფიცირებას, ფორმალიზებას, ანალიზსა და საფრთხეების მინიმიზაციისთვის საჭირო ღონისძიებების დაგეგმვას;

- ადგენს მკაფიო კრიტერიუმებს ინფორმაციული უსაფრთხოების რისკების იდენტიფიცირების, ანალიზისა და შეფასებისთვის. ეს მოიცავს რისკის დონის განსაზღვრის მეთოდოლოგიასაც;
- აქტიურად ახდენს პოტენციური ინფორმაციული უსაფრთხოების რისკების გამოვლენას. ხდება მათი მფლობელების (პასუხისმგებელი პირების) დადგენა, რისკების პოტენციური გავლენის ანალიზი ბანკზე და მათი ალბათობის შეფასება;
- გამოვლენილი რისკების შესამცირებლად, ბანკი ირჩევს და ნერგავს შესაბამის კონტროლის მექანიზმებს. ამასთან, საზღვრავს მისაღები რისკის დონეს, რაც უზრუნველყოფს, რომ მიღებული ზომები იყოს ეფექტური და პროპორციული;
- მუშავდება დეტალური რისკების მოპყრობის გეგმა, რომელიც აღწერს კონკრეტულ ნაბიჯებს, რესურსებსა და ვადებს გამოვლენილი რისკების სამართავად.
- განსაზღვრული პერიოდულობით ბანკი ახდენს ინფორმაციული უსაფრთხოებისა და კიბერ რისკის შესახებ ანგარიშგების შემუშავებასა და უფლებამოსილი ორგანოსთვის წარდგენას.

9. მომწოდებლისა და მესამე მხარის რისკების მართვა

ბანკი უზრუნველყოფს მესამე მხარეებთან ურთიერთობების უსაფრთხოებას, რათა დაიცვას ინფორმაციული აქტივები და შეამციროს მასთან დაკავშირებული რისკები. ამ მიზნით, ბანკი ახორციელებს შემდეგ აქტივობებს:

- ყველა მომწოდებელი და კონტრაქტორი, რომლებსაც აქვთ წვდომა ბანკის სენსიტიურ ინფორმაციაზე ან სისტემებზე, გადის უსაფრთხოების სრულფასოვან შეფასებას. ეს შეფასება მიზნად ისახავს მათი უსაფრთხოების მდგომარეობის შემოწმებას და ბანკის ინფორმაციული უსაფრთხოების მოთხოვნებთან შესაბამისობის უზრუნველყოფას;
- ბანკი ითვალისწინებს, რომ ყველა მესამე მხარის კონტრაქტი შეიცავდეს მკაფიო უსაფრთხოების მოთხოვნებს. ეს მოთხოვნები ავალდებულებს მომწოდებელს დაიცვას ბანკის უსაფრთხოების პოლიტიკა, მათ შორის მონაცემთა დაცვის, ინციდენტების შესახებ ანგარიშგების და სისტემის უსაფრთხოების სტანდარტები;
- მესამე მხარის მიერ უსაფრთხოების ზომების შესრულება კონტროლდება ბანკში დადგენილი პერიოდულობით. ეს უზრუნველყოფს მოწოდებული მომსახურების უწყვეტ შესაბამისობას ბანკის მოთხოვნებთან;
- ბანკში მოქმედებს დოკუმენტი „აუთსორსინგის წესები და პირობები“ რომლითაც რეგულირდება აუთსორსერებთან დაკავშირებული საკითხები.

10. ბიზნეს უწყვეტობის მართვა

ბანკი, ინფორმაციული უსაფრთხოების ასპექტების გათვალისწინებით, განსაზღვრავს ბიზნეს უწყვეტობის მოთხოვნებს. ამის საფუძველზე, ინფორმაციული უსაფრთხოების მოთხოვნების შესაბამისად, ბანკი შეიმუშავებს და მხარს უჭერს უწყვეტობის გეგმებს. ეს გეგმები ბანკს საშუალებას აძლევს, კრიზისული სიტუაციების ან კატასტროფების დროს, მოკლე დროში აღადგინოს ყველა საჭირო სერვისი.

ინფორმაციული უსაფრთხოების მართვის სისტემის მიზნებისთვის, ბანკი განსაზღვრავს და წინასწარ დადგენილი პერიოდულობით აფასებს:

- ინფორმაციული უსაფრთხოებისა და უწყვეტობის კრიტერიუმებს;
- როლებსა და პასუხისმგებლობებს მსხვილი ინციდენტის დადგომისას;
- პროცედურებს საგანგებო სიტუაციებში მოქმედებისთვის;
- სერვისის ხელმისაწვდომობის სამიზნე მაჩვენებლებს;
- ბანკში პერიოდულად ახლდება ინფორმაციის მართვის სტრატეგია, რომლის განახლების დროს მხედველობაში მიიღება კანონმდებლობის, შიდა ნორმატიული აქტების მოთხოვნები, ბანკის ბიზნეს პროცესების მფლობელების მოთხოვნები, აგრეთვე, შემდეგი კრიტერიუმები ინფორმაციასთან მიმართებაში - კონფიდენციალურობა, მთლიანობა, ხელმისაწვდომობა და აქტუალურობა.

ხელმისაწვდომობის მაღალი ხარისხის მისაღწევად, ბანკი უზრუნველყოფს ინფორმაციის დამუშავების დუბლირებული საშუალებების დანერგვას და მაღალმდგრადობის მეთოდების გათვალისწინებას ინფრასტრუქტურის დაგეგმვისა და განვითარებისას.

გარდა ამისა, ბანკში წელიწადში ორჯერ ტარდება ბიზნეს უწყვეტობის გეგმების ტესტირება, რომელიც რეგულირდება „ბიზნეს უწყვეტობის პოლიტიკით“.

11. ინფორმაციული უსაფრთხოების ინციდენტების მართვა

ბანკი უზრუნველყოფს ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცესის ეფექტიან და უწყვეტ განხორციელებას. ამ პროცესს ხელმძღვანელობს შესაბამისი გუნდი, რომლებიც პასუხისმგებლები არიან ინციდენტებზე დროულ და კოორდინირებულ რეაგირებაზე. ინფორმაციული უსაფრთხოების ყველა ინციდენტი აღირიცხება და მუშავდება ბანკში დადგენილი წესის შესაბამისად. ინფორმაციული უსაფრთხოების ინციდენტების მართვის პროცესი მოიცავს ინციდენტის იდენტიფიცირების, რეაგირების, ჩანაწერების შეგროვების, აღმოფხვრის, განხილვის და ცოდნის გაზიარების ეტაპებს. ბანკი უზრუნველყოფს ინციდენტების შესახებ დაინტერესებულ მხარეებთან კომუნიკაციას ბანკში განსაზღვრული წესების შესაბამისად.

12. ფიზიკური უსაფრთხოება

ბანკი უზრუნველყოფს ფიზიკური უსაფრთხოების მაღალ დონეს ინფორმაციული აქტივების დასაცავად. ბანკის შესაბამისი სამმართველოები ახორციელებენ შემდეგ კონტროლს:

- აკონტროლებენ მატერიალური აქტივების დაცვას, რათა თავიდან აიცილონ არაავტორიზებული წვდომა, ჩარევა ან/და დაზიანება;
- უზრუნველყოფენ ფიზიკური წვდომის კონტროლს იმ მოწყობილობებზე, რომლებიც შეიცავს ან ამუშავებს მაღალი კრიტიკულობის ან/და მგრძნობელობის ინფორმაციას. ასეთი მოწყობილობები განთავსებული უნდა იყოს ფიზიკურად დაცულ ადგილას, შეზღუდული წვდომით;

- უზრუნველყოფენ კომპიუტერული სისტემებისა და ქსელების დაცულობას ფიზიკური, ტექნიკური და პროცედურული უსაფრთხოების კონტროლის მექანიზმების გამოყენებით.

13. კორპორაციული ქსელის უსაფრთხოება

ბანკი უზრუნველყოფს ქსელური უსაფრთხოების მაღალ დონეს, რათა დაიცვას ინფორმაციული აქტივები და შეამციროს კიბერრისკები. ამ მიზნით ხორციელდება შემდეგი ძირითადი აქტივობები:

- კრიტიკული სისტემები (მაგ., ძირითადი საბანკო აპლიკაციები, მომხმარებელთა მონაცემთა ბაზები) დაყოფილია იზოლირებულ ქსელურ სეგმენტებად;
- დისტანციურად მომუშავე ან/და სისტემებზე დაშორებული ლოკაციებიდან წვდომის მქონე თანამშრომლები იყენებენ ძლიერი დაშიფვრის მქონე VPN-ებს, რათა უზრუნველყოფილი იყოს ბანკის შიდა ქსელთან უსაფრთხო კავშირი;
- ქსელურ მოწყობილობებსა და სისტემებში არსებული დაუცველობები რეგულარულად სკანირდება და ხდება მათი აღმოფხვრა, რათა თავიდან იქნას აცილებული მავნე აქტორების მიერ მათი ექსპლუატაცია.

გარდა ამისა, ბანკში წელიწადში ორჯერ ტარდება ბიზნეს უწყვეტობის ტესტირება, რომლის ფარგლებში ბანკი ახორციელებს შიდა კორპორაციული ქსელის უწყვეტი მუშაობის ტესტირებას, როგორც ძირითად, ასევე, ალტერნატიულ სასერვერო ინფრასტრუქტურაში.

14. აუდიტი და შესაბამისობა

ბანკი, დადგენილი პერიოდულობით, ატარებს ინფორმაციული უსაფრთხოების მართვის სისტემის აუდიტს, რათა უზრუნველყოს უსაფრთხოების მოთხოვნებთან სრული შესაბამისობა და მუდმივი გაუმჯობესება. აუდიტის მიზანია გამოავლინოს:

- ბანკის შესაბამისობა საქართველოს ეროვნული ბანკის მოთხოვნებთან, საერთაშორისო სტანდარტებთან (მაგ., ISO ISO/IEC 27001, COBIT და სხვა.) და ბანკის შიდა მოთხოვნებთან;
- რამდენად შეესაბამება არსებული უსაფრთხოების ზომები და პროცესები დადგენილ ინფორმაციული უსაფრთხოების მოთხოვნებს;
- იუმს-ის დანერგვისა და შემდგომი მხარდაჭერისთვის საჭირო გაუმჯობესების შესაძლებლობები;
- აუდიტის შერჩევისა და ჩატარების პროცესში ბანკის მიერ გათვალისწინებულია „კომერციულ ბანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელოს“ მოთხოვნები.

15. დაუცველობის მართვა

ბანკი ახორციელებს დაუცველობის მართვის უწყვეტ და რეგულარულ პროცესს, რათა დროულად მოახდინოს დაუცველობის იდენტიფიცირება, შეფასება, აღმოფხვრა და მონიტორინგი. დაუცველობის მართვის პროცესი მოიცავს შემდეგ ძირითად ეტაპებს:

- დაუცველობის სკანირება ტარდება რეგულარული პერიოდულობით ბანკის ყველა ქსელურ მოწყობილობაზე, სერვერზე, სამუშაო სადგურზე და აპლიკაციაზე;
- ტარდება კონფიგურაციის აუდიტი, კოდის უსაფრთხოების მიმოხილვა და სხვა ტექნიკური შემოწმებები, რათა გამოვლინდეს ცნობილი სისუსტეები და კონფიგურაციის შეცდომები;
- მუდმივად ხდება გარე საფრთხეების შესახებ ინფორმაციის (მაგ., CVE) მონიტორინგი, რათა დროულად მოხდეს რეაგირება ახლად აღმოჩენილ დაუცველობებზე;
- იდენტიფიცირებული დაუცველობები ფასდება მათი სიმძიმის, ექსპლუატაციის სირთულის და პოტენციური გავლენის მიხედვით ბანკის აქტივებზე, ოპერაციებსა და რეპუტაციაზე;
- ბანკი იყენებს რისკზე დაფუძნებულ მიდგომას, რათა განისაზღვროს აღმოფხვრის პრიორიტეტები, უპირატესობა ენიჭება ყველაზე კრიტიკულ და მაღალი რისკის მქონე სისუსტეებს;
- უსაფრთხოების პაჩები და განახლებები ოპერაციული სისტემებისთვის, აპლიკაციებისთვის და firmware-სთვის გამოიყენება დაუყოვნებლივ, დამტკიცებული პროცედურებისა და რისკზე დაფუძნებული პრიორიტეტების შესაბამისად;
- ბანკში დაუცველობის მართვის პროცესი და აღმოფხვრის პროგრესი მუდმივად კონტროლდება;
- რეგულარული ანგარიშები დაუცველობის სტატუსის, აღმოფხვრის ეფექტიანობისა და საერთო რისკების შესახებ წარედგინება ინფორმაციული უსაფრთხოების სამუშაო ჯგუფს.

16. მედია მატარებლების უსაფრთხოდ გამოყენება

ბანკი უზრუნველყოფს, რომ ყველა გამოყენებული მედია მატარებელი, რომელიც შეიცავს სენსიტიურ ინფორმაციას, იყოს უსაფრთხოდ მართული მისი მთელი სასიცოცხლო ციკლის განმავლობაში - შექმნიდან განადგურებამდე. ამ მიზნით:

- ბანკში არსებული ყველა მედია მატარებელი, რომელიც შეიცავს სენსიტიურ ინფორმაციას (მაგ., გარე მყარი დისკები, USB და სხვა) არის აღრიცხული და მარკირებული განსაზღვრული წესების შესაბამისად;
- მედია მატარებლებზე განთავსებული ინფორმაცია კლასიფიცირებულია ბანკში შემუშავებული პოლიტიკის მიხედვით;
- ბანკში განსაზღვრულია ინფორმაციის უსაფრთხოდ დამუშავების, შენახვისა და განადგურების მოთხოვნები;
- მედია მატარებლები, რომლებიც შეიცავენ სენსიტიურ ინფორმაციას, შენახულია უსაფრთხო გარემოში, ფიზიკური დაშვების მკაცრი კონტროლის ქვეშ, რათა თავიდან იქნას აცილებული არაავტორიზებული წვდომა, დაზიანება ან/და ქურდობა;

- წვდომა მედია მატარებლებზე, რომელიც შეიცავს სენსიტიურ ინფორმაციას, შემოიფარგლება მხოლოდ მინიმალური დაშვების პრინციპით;
- ნებისმიერი მედია მატარებელი, რომელიც განკუთვნილია სარეზერვო ასლების ან აღდგენის მიზნებისთვის, უნდა იყოს რეგულარულად ტესტირებული, რათა უზრუნველყოფილი იყოს მისი გამართული ფუნქციონირება და ინფორმაციის ხელმისაწვდომობა.

17. ინფორმაციულ სისტემაში შეღწევადობის ტესტირება

ბანკი, დადგენილი პერიოდულობით, ატარებს ინფორმაციული სისტემების შეღწევადობის ტესტირებას. ამ ტესტირების მთავარი მიზანია ბანკის სისტემებში არსებული არასწორი კონფიგურაციების, დაუცველობების ან/და სისუსტეების გამოვლენა.
შეღწევადობის ტესტირების შედეგად იდენტიფიცირებული ყველა სისუსტისა და შეუსაბამობის აღმოსაფხვრელად, ბანკი ამზადებს დეტალურ სამოქმედო გეგმას და უზრუნველყოფს ამ პროცესის ეფექტიან განხორციელებას, მონიტორინგს და ანგარიშგებას, რათა სისტემების უსაფრთხოების დონე გაუმჯობესდეს.

18. ცნობიერების ამაღლება და ტრენინგები

ბანკი აქტიურად ზრუნავს თანამშრომელთა ინფორმაციული უსაფრთხოების ცნობიერების ამაღლებაზე. ამ მიზნით:

- ყველა დასაქმებული პერსონალი ინფორმირებულია ინფორმაციული უსაფრთხოების პოლიტიკებისა და დამხმარე დოკუმენტაციის შესახებ. განსაკუთრებული აქცენტი კეთდება მათ პასუხისმგებლობებსა და როლზე ინფორმაციული უსაფრთხოების მართვის სისტემის ეფექტიანობის უზრუნველყოფაში;
- ბანკის ყველა თანამშრომელი გადის ცნობიერების ამაღლების ტრენინგს და შესაბამის ტესტირებას წელიწადში ორჯერ. ეს უზრუნველყოფს უსაფრთხოების უახლესი საფრთხეებისა და საუკეთესო პრაქტიკებზე ცოდნის მუდმივ განახლებას;
- ყველა საჭირო საინფორმაციო მასალა და დოკუმენტაცია მუდმივად ხელმისაწვდომია ბანკის ინტრანეტზე, რაც თანამშრომლებს საშუალებას აძლევს, ნებისმიერ დროს გაეცნონ უსაფრთხოების წესებს და განაახლონ შესაბამისი ცოდნა.

19. მუდმივი გაუმჯობესების ციკლი

ბანკი აქტიურად ახორციელებს ინფორმაციული უსაფრთხოების მართვის სისტემის მუდმივ გაუმჯობესებას. ამ პროცესისთვის გამოიყენება მრავალი წყარო, მათ შორის:

- აუდიტის შედეგები, როგორც შიდა, ისე გარე აუდიტების დასკვნები;
- არსებული ხარვეზების აღმოფხვრა და მომავალი რისკების პრევენცია;
- რეგულარული რისკების იდენტიფიცირება და ანალიზი;
- მომხდარი ინციდენტებიდან მიღებული გაკვეთილები (Lessons learned);
- სისტემური მოვლენების უწყვეტი ანალიზი;
- უმაღლესი ხელმძღვანელობის მიერ პერიოდული განხილვები და შეფასებები.

ამ მონაცემების საფუძველზე, ბანკი აყალიბებს დეტალურ გაუმჯობესების გეგმებსა და მიზნებს. პროგრესის შესახებ ანგარიში, კვარტალში ერთხელ, წარედგინება ინფორმაციული უსაფრთხოების სამუშაო ჯგუფს განსახილველად და დასამტკიცებლად, რაც უზრუნველყოფს იუმს-ის უწყვეტ განვითარებას და ეფექტიანობას.

20. პოლიტიკის დარღვევა

ბანკის ინფორმაცია, ინფორმაციული სისტემები და ტექნოლოგიები წარმოადგენენ ბანკის საქმიანობის მნიშვნელოვან კომპონენტებს. შესაბამისად, ბანკის ყველა თანამშრომელი ვალდებულია უზრუნველყოს აღნიშნული რესურსების უსაფრთხოება, კონფიდენციალურობის, ხელმისაწვდომობისა და მთლიანობის თვალსაზრისით. ბანკის სხვადასხვა პროფესიულ პრაქტიკასთან და დადგენილ პოლიტიკასთან შეუსაბამობა შესაძლოა ჩაითვალოს მნიშვნელოვან დარღვევად, რამაც შეიძლება გამოიწვიოს დისციპლინური პასუხისმგებლობა, მათ შორის, შრომითი ურთიერთობის ან ხელშეკრულების შეწყვეტა მოქმედი კანონმდებლობის შესაბამისად.

21. პოლიტიკის გადახედვის გეგმა

პოლიტიკის გადახედვას, განახლებას, მუდმივ გაუმჯობესებას და მის შესაბამისობას ბანკის მიზნებთან მიმართებაში უზრუნველყოფს ბანკის უსაფრთხოების სამმართველოს ინფორმაციული უსაფრთხოების მენეჯერი. პოლიტიკა უნდა გადაიხედოს არანაკლებ 3 წელიწადში ერთხელ ან/და მნიშვნელოვანი ცვლილებების შემთხვევაში.

იმ შემთხვევაში, თუ დოკუმენტში განხილულ საკითხებთან დაკავშირებით, საქართველოს კანონმდებლობაში ან/და მარეგულირებელი ორგანოს ნორმატიულ აქტებში შევიდა ცვლილება, უპირატესობა ენიჭება ზემოთ ხსენებულ დოკუმენტებს. დოკუმენტი ან/და მასში შეტანილი ნებისმიერი ცვლილება მტკიცდება ბანკის სამეთვალყურეო საბჭოს მიერ, ბანკში მოქმედი წესის შესაბამისად.