ბანკის ვებგვერდზე https://www.tbcbank.ge/web/ka/web/guest/card-payments **განთავსებული "ელექტრონული კომერციის მომსახურების შესახებ ხელშეკრულების ძირითადი პირობების" 1.4. პუნქტის შესაბამისად, სს "თიბისი ბანკი" გთავაზობთ "ელექტრონული კომერციის მომსახურების შესახებ ხელშეკრულების სტანდარტულ პირობებში" (შემდგომში "სტანდარტული პირობები") შემდეგი ცვლილებების / დამატებების შეტანას:**

- **სტანდარტულ პირობებს დაემატოს დანართი #4 შემდეგი რედაქციით:**

„დანართი #4
პერსონალურ მონაცემთა დამუშავების პოლიტიკა

1.1. კომპანია აცხადებს და იძლევა გარანტიას, რომ:

1.1.1. წინამდებარე ხელშეკრულებითა და საქართველოს კანონმდებლობით განსაზღვრული, მასზე გადაცემულ პერსონალურ მონაცემებს დაამუშავებს მხოლოდ წინამდებარე ხელშეკრულების ფარგლებში კონკრეტული მიზნის მისაღწევად და მოქმედი კანონმდებლობის შესაბამისად;

1.1.2. პერსონალურ მონაცემთა არაავტორიზებული დამუშავების (მათ შორის შემთხვევითი ან უნებართვო გავრცელება, წვდომა, შეცვლა და განადგურება) აღსაკვეთად გაატარებს შესაბამის ტექნიკურ და ორგანიზაციულ ზომებს პერსონალურ მონაცემთა ბუნებისა და პერსონალურ მონაცემთა სუბიექტებთან დაკავშირებული რისკების გათვალისწინებით;

1.1.3. შეზღუდავს პერსონალურ მონაცემებთან წვდომის უფლების მქონე პირთა წრეს და ასეთ უფლებას მიანიჭებს მხოლოდ იმ პირებს, რომლებიც უშუალოდ საჭიროებენ მონაცემებზე წვდომას და რომელთაც გააზრებული აქვთ მონაცემთა კონფიდენციალურობისა და უსაფრთხოების დაცვის ვალდებულება;

1.1.4. პერსონალურ მონაცემებზე შემთხვევითი ან უნებართვო წვდომის, ასეთი მონაცემების განადგურების, დაკარგვის, შეცვლის ან გასაჯაროვების შემთხვევაში დაუყოვნებლივ, თუმცა არაუგვიანეს ასეთი შემთხვევის დადგომიდან 2 (ორი) სამუშაო დღისა, შეატყობინებს ბანკს შემთხვევის შესახებ ინციდენტის ბუნებისა და გამჟღავნებული/განადგურებული/შეცვლილი პერსონალური მონაცემების მითითებით;

1.1.5. დაუყოვნებლივ მიიღებს ზომებს ინციდენტზე დროული რეაგირებისა და მისი გამომწვევი მიზეზების აღმოფხვრისთვის და გატარებული ზომების შესახებ აცნობებს ბანკს;

1.1.6. ბანკის წინასწარი თანხმობის გარეშე მესამე პირს არ გადასცემს ხელშეკრულების ფარგლებში ბანკისგან მიღებულ პერსონალურ მონაცემებს. ასეთი თანხმობის მოპოვების შემთხვევაში, მონაცემთა მიმღებ მესამე პირზე ყოველგვარი შეზღუდვის გარეშე გავრცელდება წინამდებარე პოლიტიკით განსაზღვრული მოთხოვნები;

1.1.7. მხოლოდ განსაზღვრულ შემთხვევებში და ბანკის წინასწარი წერილობითი თანხმობის შესაბამისად პერსონალური მონაცემების დამუშავების პროცესში ჩართავს ქვე-კონტრაქტორებს, რომლებზეც ყოველგვარი შეზღუდვის გარეშე გავრცელდება წინამდებარე პოლიტიკით განსაზღვრული პირობები. მონაცემთა დამუშავების პროცესში ქვე-კონტრაქტორის ჩართვა არ ათავისუფლებს მას ნაკისრი ვალდებულებებისაგან და არ ზღუდავს მისი პასუხისმგებლობის ფარგლებს ასეთი ვალდებულებების დარღვევისას დამდგარ ზიანთან მიმართებაში;

1.1.8. წინამდებარე პოლიტიკის 1.1.7 მუხლით განსაზღვრული უფლების გამოყენების შემთხვევაში, ბანკს შეატყობინოს ხელშეკრულების ხელმოწერის დროისთვის დაქირავებული ქვე-კონტრაქტორების ვინაობა და მათთან დაკავშირებული ნებისმიერი ცვლილება განახორციელოს მხოლოდ ბანკის წინასწარი წერილობითი თანხმობით. ბანკი უფლებამოსილია, არ დაეთანხმოს ხელშემკვრელი მხარის მიერ წამოყენებული ქვე-კონტრაქტორის კანდიდატურას. იმ შემთხვევაში, თუ აღნიშნული საკითხი ვერ გადაწყდება მოლაპარაკების გზით, ბანკი უფლებამოსილია ყოველგვარი ზიანის ანაზღაურების გარეშე ვადამდე შეწყვიტოს მხარესთან დადებული ხელშეკრულების მოქმედება;

1.1.9. ბანკის მიერ პოლიტიკის 1.1.8 მუხლის საფუძველზე ხელშეკრულების შეწყვეტის შემთხვევაში, გონივრულ ვადაში დაუბრუნოს ბანკს და აღდგენის შესაძლებლობის გარეშე წაშალოს/გაანადგუროს მისთვის გადაცემული პერსონალური მონაცემები და მათი ასლები. ბანკი უფლებამოსილია, მხარეს მოსთხოვოს მონაცემთა წაშლის დადასტურება. წინამდებარე მუხლი არ ვრცელდება ისეთ ინფორმაციაზე, რომლის შენახვის ვალდებულებას მხარეს მოქმედი კანონმდებლობა ანიჭებს.

1.1.10. პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული ვალდებულებები ძალაში რჩება მხარეთა შორის სახელშეკრულებო ურთიერთობის შემდეგ იმ ვადით, რა ვადითაც მხარე ინარჩუნებს წვდომას ხელშემკვრელი მხარის მიერ მისთვის გადაცემულ პერსონალურ მონაცემებზე. წინამდებარე მუხლი არ უნდა იქნას მიჩნეული კომპანიის უფლებად, შეინარჩუნოს წვდომა ხელშეკრულების საფუძველზე მიღებულ პერსონალურ მონაცემებზე სახელშეკრულებო ურთიერთობის დასრულების შემდეგ. კომპანია ვალდებულია, სახელშეკრულებო ურთიერთობის დასრულებიდან გონივრულ ვადაში, მაგრამ არაუგვიანეს 30 დღისა დააბრუნოს და აღდგენის შესაძლებლობის გარეშე წაშალოს/გაანადგუროს მისთვის ბანკსი მიერ გადაცემული პერსონალური მონაცემები და მათი ასლები;

1.2. ბანკი უფლებამოსილია, გონივრული ეჭვის არსებობისას, შეამოწმოს ხელშემკვრელი მხარისთვის ბანკის მიერ გადაცემული პერსონალური მონაცემების დამუშავების პროცესში გამოყენებული საშუალებებისა და სისტემების გამართულობა; ასევე, მათი ტექნიკური და ორგანიზაციული მახასიათებლების შესაბამისობა წინამდებარე პოლიტიკით დადგენილ უსაფრთხოების მოთხოვნებთან;
1.3. ზემოაღნიშნული გარანტიების დარღვევის სიმძიმიდან გამომდინარე, ბანკს აქვს უფლება, შემოწმების მიზნით, ხელშემკვრელ მხარეს მოსთხოვოს შესაბამისი ინფორმაციისა და დოკუმენტაციის ბანკისთვის წარდგენა.
1.4. ბანკი სრულად იხსნის პასუხისმგებლობას ნებისმიერ ზიანსა და ხარჯზე, რომელიც გამოწვეულია ხელშემკვრელი მხარის მიერ წინამდებარე პოლიტიკით განსაზღვრული რომელიმე ვალდებულების განზრახი ან გაუფრთხილებელი დარღვევით;
1.5. მონაცემების დამმუშავებელი მხარე ვალდებულია სრულად დაიცვას წინამდებარე ხელშეკრულების დანართში მითითებული ინფორმაციული სისტემების ინფრასტრუქტურის მოთხოვნები.

დანართი: ინფორმაციული სისტემების ინფრასტრუქტურის მოთხოვნები

ხელშემხვრელი მხარის გარემო რომელშიც დროებით ან მუდმივად ხვდება ბანკის მიერ მიწოდებული პერსონალური მონაცემები საჭიროა უზრუნველყოფილი იყოს შემდეგი:
1. პერსონალური მონაცემების შესანახად და დასამუშავებლად უნდა არსებობდეს იზოლირებული გარემო რომელიც ძირითადი ინფრასტრუქტურისგან იქნება გამოყოფილი დამოუკიდებელი Firewall ით.
2. გარემოს Firewall-ზე წვდომების დაშვება უნდა კონტროლდებოდეს შესაბამისი უფლებამოსილი პირების მიერ.
3. იზოლირებულ გარემოში მოთავსებულ ინფორმაციასთან წვდომა უნდა ხორციელდებოდეს ს.წ. ტერმინალ სერვერების (Jump Server) საშუალებით
4. უნდა კონტროლდებოდეს და ხორციელდებოდეს გარემოს მთლიანობის/წვდომადობის მონიტორინგი
5. გარემოში მოთავსებული სერვერებზე უნდა ხორციელდებოდეს განახლებების მონიტორინგი
6. სადაც შესაძლებელია პერსონალური მონაცემები უნდა ინახებოდეს დაშიფრული სახით ძლიერი შიფრაციის ალგორითმების გამოყენებით
7. იზოლირებულ გარემოსთან წვდომა უნდა ხორციელდებოდეს დაცული მეთოდით, დაშიფრული კომუნიკაციით და უსაფრთხო პროტოკოლის გამოყენებით
8. იზოლირებული გარემოსთვის უნდა არსებობდეს პაროლების პოლიტიკა რომელიც განსაზღვრას პაროლის სირთულეს, ცვლილების დროს და ისტორიას
9. იზოლირებულ გარემოს სერვერებზე ადმინ მომხმარებლების პაროლები უნდა იყოს დანაწევრებული მინიმუმ ორ ნაწილად და უნდა ინახებოდეს სხვადასხვა მფლობელთან, უსაფრთხო მეთოდის გამოყენებით
10. გარემოზე წვდომის დაშვებისას უნდა ხორციელდებოდეს მომხმარებლის ორ ნაბიჯიანი ავთენტიფიკაცია (ე.წ. Two Step Authentication)
11. იზოლირებული გარემო არ უნდა იყოს ინტერნეტიდან წვდომადი
12. იზოლირებულ გარემოს სერვერებზე უნდა ხორციელდებოდეს ლოგირება, ლოგი უნდა ინახებოდეს ცენტრალიზებულად და საჭიროების შემთხვევაში მოხდეს მისი გამოყენება ინციდენტის ან ხარვეზის გამოკვლევის პროცესში
13. პერსონალური მონაცემების შესანახად დასამუშავებლად ან გადასაცემად არ უნდა გამოიყენებოდეს ღრუბლოვანი გარემო (Remote storage, Cloud Service)
14. დეველოპმენტის ან ტესტირების ფარგლებში პერსონალური მონაცემების გამოყენებისას უნდა ხდებოდეს ინფორმაციის დამახინჯება ისეთი სახით რომ ვერ ხდებოდეს პიროვნების პირდაპირი ან ირიბი იდენტიფიცირება
15. ხანდაზმულობით ან სპეციალური მოთხოვნით ინფორმაციის განადგურებისას გამოყენებულ უნდა იქნას შრედერი ან ცეცხლი. განადგურების პროცესს უნდა ესწრებოდეს წინასწარ განსაზღვრული ბანკის წარმომადგენელი.“