მოვაჭრის უსაფრთხოების პოლიტიკა	Trader's Security Policy
1. მიზანი	**1. The Purpose**
უსაფრთხოების პოლიტიკის მიზანია მოვაჭრის კონტროლს ქვეშ არსებული ინფორმაციის დასაცავად კონტროლის მექანიზმების შექმნა და მისი მეშვეობით კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველყოფა.	The purpose of the security policy is to create control mechanisms to protect the information under the trader's control and thereby ensure confidentiality, integrity and availability.
პოლიტიკა მიზნად ისახავს შიდა და გარე საფრთხეების მიმართ ინფორმაციული უსაფრთხოების დამცავი მექანიზმების, კრიზისული სიტუაციებისა და განზრახ დაზიანებების წინააღმდეგ ქცევის ძირითადი წესების შექმნას.	The policy aims to create information security protection mechanisms against internal and external threats, basic rules of behavior against crisis situations and intentional injuries.
2. უსაფრთხოების პოლიტიკის სუბიექტები	**2. Security Policy Entities**
2.1. უსაფრთხოების პოლიტიკის მოთხოვნები ვრცელდება:	2.1. Security policy requirements apply to:
ა) მოვაჭრის მიერ დაქირავებულ პირებზე – შემდგომში „სუბიექტები“;	a) persons hired by the trader – hereinafter "Subjects";
ბ) ყველა პირზე, რომელსაც შესაძლოა ჰქონდეს წვდომა მოვაჭრის მიერ დაცულ ინფორმაციასთან.	b) to all persons who may have access to information protected by the merchant.
2.2. სუბიექტები ვალდებულნი არიან დაიცვან პოლიტიკის მოთხოვნები და აიღონ პასუხისმგებლობა მათთვის დაწესებული სტანდარტებისა და წესების სრულყოფილად და ზედმიწევნით შესრულებაზე.	2.2. Entities are obliged to comply with the requirements of the policy and take responsibility for the complete and thorough implementation of the standards and rules set for them.
3. უსაფრთხოების მიზნით გასატარებელი ღონისძიებები	**3. Safety measures**
3.1. მოვაჭრე ახორციელებს მუდმივ კონტროლს ინფორმაციის დამამუშავებელ მოწყობილობებზე მათი სწორი და უსაფრთხო სარგებლობის უზრუნველყოფის მიზნით.	3.1. The trader carries out continuous control over the information processing devices in order to ensure their correct and safe use.
3.2. მოვაჭრე უზრუნველყოფს ინფორმაციის დამამუშავებელი სისტემების დოკუმენტაციის შექმნას, მათ შორის, გამოყენებული ტექნოლოგიების კონფიგურაციების ჩათვლით. ინფორმაცია, რომელიც შეიცავს ინფორმაციული უსაფრთხოებისათვის მნიშვნელოვან მონაცემებს, შეინახება უსაფრთხო ადგილას და ინფორმაციის მიღების აუცილებლობის მიხედვით შეიზღუდება მასზე წვდომა.	3.2. The trader shall ensure the creation of documentation of the information processing systems, including the configurations of the technologies used. Information that contains data important for information security will be stored in a safe place and access to it will be restricted depending on the need to receive information.
3.3. ინფორმაციული მატარებლები, რომლებიც შეიცავენ ინფორმაციული კლასიფიკაციიდან გამომდინარე მაღალი	3.3. Information carriers containing highly critical information based on information classification

კრიტიკულობის მქონე ინფორმაციას, აღიწერება და მათი გამოყენება, შენახვა და განადგურება დაექვემდებარება მკაცრ კონტროლს.	will be recorded and their use, storage and destruction will be subject to strict control.
3.4. სუბიექტები ვალდებულნი არიან ნებისმიერი კომპიუტერული პროგრამის გამოყენებამდე დარწმუნდნენ, რომ პროგრამების გამოყენება არ გამოიწვევს ვირუსების გავრცელებას და ტექნიკური მოწყობილობების იმგვარ დაზიანებას, რაც საფრთხის ქვეშ დააყენებს ინფორმაციის დაცულობას.	3.4. Subjects are obliged to make sure before using any computer program that the use of the program will not lead to the spread of viruses and damage to the technical equipment, which would endanger the security of information.
3.5. მოვაჭრის მიერ მუდმივად უნდა ხორციელდებოდეს სუბიექტების სწავლება/დატრენინგება, რათა თავიდან იქნას აცილებული ნებისმიერი შეცდომა ინფორმაციის უსაფრთხოებასთან დაკავშირებით.	3.5. The trader should continuously educate/train the subjects to avoid any mistakes related to information security.
3. რისკის შეფასება და მართვა	**3. Risk assessment and management**
3.1. რისკის შეფასება არის ამოსავალი წერტილი უსაფრთხოების მართვის ნებისმიერი გეგმის შემუშავებამდე. რისკის შეფასება განსაზღვრავს არსებული და პროგნოზირებადი უსაფრთხოების რისკებს, რომლებიც დაკავშირებულია პროექტთან/ ოპერაციებთან.	3.1. Risk assessment is the starting point before any safety management plan is developed. Risk assessment identifies existing and foreseeable security risks associated with the project / with operations.
3.2. რისკების შეფასების გადახედვა მოხდება ყოველწლიურად ან რაიმე მნიშვნელოვანი უსაფრთხოებასთან დაკავშირებული შემთხვევისას. რისკების შეფასება ასევე გადაიხედება მასთან დაკავშირებული კანონმდებლობის ნებისმიერი ცვლილებისას.	3.2. The risk assessment will be reviewed annually or upon any significant safety-related incident. The risk assessment will also be revised in case of any changes in the relevant legislation.
რისკების შეფასებისას გათვალისწინებული/დაცული უნდა იყოს შემდეგი საკითხები: 3.3 რეგულარულად ჩატარდეს ვებ-საიტის დაცვის სისტემების შეფასება, რათა დროულად გამოვლინდეს ნებისმიერი სისტემური ხარვეზი და აღმოიფხვრას იგი. 3.4. დარწმუნდეს, რომ საგადახდო სერვისის პროვაიდერი შეესაბამება PCI DSS-ს, რომელიც მოიცავს უსაფრთხო ქსელის შენარჩუნებას, ბარათის მფლობელის მონაცემების დაცვას, ქსელების რეგულარულ მონიტორინგს და	During the risk assessment, the following issues should be taken into consideration: 3.3. Regularly conduct vulnerability assessments on the website and associated systems to identify potential security weaknesses or loopholes that could be exploited by attackers. 3.4. Ensure that payment service provider is compliant with the PCI DSS, which includes maintaining a secure network, protecting cardholder data, regularly monitoring and testing networks, and implementing strong access control measures.

ტესტირებას და წვდომის კონტროლის ძლიერი ზომების განხორციელებას. 3.5. დაინერგოს უსაფრთხო პროტოკოლები, როგორიცაა HTTPS, ბარათის მფლობელის მონაცემების ინტერნეტით გადასაცემად, რათა დაიცვათ არაავტორიზებული ჩარევისგან ან წვდომისგან. 3.6. გამოყენებულ იქნას დაშიფვრის ძლიერი მექანიზმები (მაგ. SSL/TLS) სენსიტიური მონაცემების, მათ შორის საკრედიტო ბარათის ინფორმაციის დაშიფვრისთვის, როგორც ტრანსპორტირებისას, ასევე დასვენების დროს, რათა თავიდან აცილებულ იქნას არაავტორიზებული წვდომა ან მონაცემთა ქურდობა. 3.7. განხორციელდეს მკაცრი წვდომის კონტროლი, რათა შეზღუდულ იქნას წვდომა ვებსაიტის მგრძნობიარე არეაზე, გადახდის დამუშავების სისტემების ჩათვლით, მხოლოდ ავტორიზებული პერსონალისთვის. ეს მოიცავს პაროლების დაცვის ძლიერ პოლიტიკას. 3.8. დარწმუნდით, რომ ვებსაიტების ყველა პროგრამული უზრუნველყოფა, კონტენტის მართვის სისტემების და დანამატების ჩათვლით, განახლებულია უსაფრთხოების უახლესი პატჩებითა და განახლებებით რისკების შესამცირებლად. 3.9. გამოყენებულ იქნას შეჭრის აღმოჩენისა და პრევენციის სისტემები (IDS/IPS) ქსელის ტრაფიკის მონიტორინგისთვის და პოტენციური თავდასხმების ან საეჭვო აქტივობების იდენტიფიცირებისთვის. განახორციელეთ ზომები ამ საფრთხეების დაბლოკვის ან შესამცირებლად რეალურ დროში. 3.10. უზრუნველყოფილ იქნას ვებსაიტის და მასთან დაკავშირებული მონაცემთა ბაზების განთავსება უსაფრთხო და რეპუტაციის მქონე ჰოსტინგის პროვაიდერზე, რომელიც	3.5. Implement secure protocols, such as HTTPS, for transmitting cardholder data over the internet to protect against unauthorized interception or access. 3.6. Use strong encryption mechanisms (e.g., SSL/TLS) to encrypt sensitive data, including credit card information, both during transit and at rest, to prevent unauthorized access or data theft. 3.7. Implement strict access controls to restrict access to sensitive areas of the website, including the payment processing systems, to authorized personnel only. This includes strong password policies. 3.8. Ensure that all website software, including content management systems, and plugins, up to date with the latest security patches and updates to mitigate risks. 3.9. Use intrusion detection and prevention systems (IDS/IPS) to monitor network traffic and identify potential attacks or suspicious activities. Implement measures to block or mitigate these threats in real-time. 3.10. Ensure hostage of the website and associated databases on a secure and reputable hosting provider that implements robust security measures, such as firewalls, intrusion detection systems, and regular security audits. 3.11. Conduct periodic security audits by independent third-party assessors to evaluate the effectiveness of the security controls and identify any potential weaknesses or areas for improvement.

ახორციელებს უსაფრთხოების მძლავრ ზომებს, როგორიცაა firewalls, შეჭრის აღმოჩენის სისტემები და რეგულარული უსაფრთხოების აუდიტი. 3.11. ჩატარდეს პერიოდული უსაფრთხოების აუდიტი დამოუკიდებელი მესამე მხარის შემფასებლების მიერ, რათა შეაფასონ უსაფრთხოების კონტროლის ეფექტურობა და გამოავლინონ ნებისმიერი პოტენციური სისუსტე ან გაუმჯობესების სფერო.	
4. პასუხისმგებლობა	**4. Responsibility**
4.1. უსაფრთხოების პოლიტიკაზე და უსაფრთხოების პოლიტიკით დადგენილი მოთხოვნების შესრულებაზე პასუხისმგებელია მოვაჭრე.	4.1. The trader is responsible for the security policy and the fulfillment of the requirements established by the security policy.
5. სხვა დებულებები	**5. Other Provisions**
5.1. უსაფრთხოების პოლიტიკა არის საჯარო და ხელმისაწვდომი მოვაჭრის ნებისმიერი მომხმარებლისთვის.	5.1. The security policy is public and accessible to any consumer of the trader.