Information Security Statement for External Parties

Version	Date	Changes	Modified by	Approved by
1.0	10.3.2024	First version	Primesec Ltd.	Ari Dobner

1. General

1.1. **Clearshift US Company, Clearshift UAB, and Clearshift Israel Ltd.** (separately and together hereinafter referred to as "The Company", "Us", and "We") redefine international payments with an innovative pricing model and transparent process that is revolutionizing the foreign currency payments market. Committed to fair pricing standards, Clearshift eliminates mark-ups, hidden costs, and surprise commissions to save you money while enabling safe and rapid global currency transactions.

1.2. The Company has offices in Israel, the United States, and Lithuania, and it provides services worldwide.

1.3. Customer data is an important asset of significant value to us and we are committed to protecting it from potential threats to disrupt business continuity or compromise the privacy of data subjects or customer data.

1.4. The protection of the confidentiality, integrity, and availability of the data we hold or process is a central principle of the Company, whether the information belongs to the Company, its employees, its partners, its customers, or its suppliers.

1.5. The Company is committed to maintaining information security through responsible management, appropriate use, and privacy protection, by the provisions of applicable legislation and agreements.

2. Management Commitment

2.1. We are committed to continuous improvement and therefore provide adequate resources to our information security plan. We build and maintain an appropriate level of information security management and budget the information security work plan accordingly. In addition, the management ensures that the resources are available and are being used appropriately.

2.2. The Company's management defines measures & objectives for examining the Company's Information Security Management System (ISMS) regularly.

2.3. The Company has appointed a Chief Information Security Officer ("CISO") who is responsible for information security issues. The CISO is responsible for controlling the information security policy and providing support and advice for its implementation. The CISO contact details are: Or Lavi; Tel: 972-54-256-6641; Email: or@primesec.co.il.

2.4. All managers in the Company are responsible for the implementation of the policy and the compliance of the personnel in their departments. Compliance with the information security policy and procedures is a duty of each of the Company's employees.

3. Policies and procedures

3.1. The Company implements organizational and technical measures to ensure a high level of information security and compliance with the requirements of the applicable legislation. These measures are reviewed and updated regularly.

3.2. Our policy ensures that:

- ✓ The needs and expectations of all involved parties are addressed.
- ✓ Information will be protected against any unauthorized access.
- ✓ The confidentiality of information will be assured.
- ✓ The integrity of information will be maintained.
- ✓ The availability of information for business processes will be maintained.
- ✓ The legislative and regulatory requirements will be met.
- ✓ The Business continuity plans will be developed, maintained, and tested.
- ✓ The information security training will be available and mandatory for all employees.
- ✓ The IT resources will be optimally utilized, and information system changes will be controlled.
- ✓ Any suspected information leak or information security breach will be reported to the CISO and thoroughly investigated.

3.3. The Company has defined procedures for implementing its information security policy, including the activation of virus control measures, data encryption methods, password and authentication policies, network architecture, and data separation architecture, all according to the requirements of accepted international cyber security standards.

3.4. Accordingly, our system implements data security "by design" and offers a rich set of features to allow customer administrators to implement the strictest security policies.

3.5. The Company performs periodic technical tests by an independent auditor and undergoes an ISO audit every year.

4. Employees' Commitment

4.1. Our employees are familiar with the Company's information security policies and procedures, committed to information security, and acknowledge the importance of implementing it in their daily work.

4.2. Our employees have knowledge and experience in the information security field.

4.3. All our employees are signed on an NDA and information security requirements.

4.4. Moreover, all our employees participate frequently in awareness training and are updated regularly with information security issues.

5. Applicable legislation, standards, and frameworks

5.1. To demonstrate our commitment to information security and privacy, we implement industry best practice security controls.

5.2. We work with information security and privacy consultants, auditors, and legal advisors to ensure ongoing compliance with standards and the applicable legislation.

5.3. Standards

- ISO 27001 - The international standard for information security that sets out the specifications for an effective ISMS (information security management system).

5.4. Legislation

- The Israeli Privacy Protection Law, 5741-1981.
- The Privacy Protection Regulations (Data Security) 5777-2017.
- The Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001.
- The Israeli Circular of Cyber risk management in financial service providers (hereinafter: "FSP Circular").
- EU General Data Protection Regulations (EU GDPR) - Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.
- US: 16 CFR Part 314 Standards for Safeguarding Customer Information (Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act).
- Bank Of Lithuania - Resolution on the Approval of the Description of Requirements for Information and Communication Technology and Security Risk Management.

- Bank Of Lithuania - Resolution on the Approval of the rules on the outsourcing of operational functions of financial market participants.
- Bank Of Lithuania - Rules Regarding Operational or Security Incident Reporting to the Bank of Lithuania.

6. Context of the organization

6.1. Understanding the organization and its context

The Company has identified the external and internal issues that affect its ability to achieve the intended outcomes of its information security management system. The Company's policies and procedures shall be defined considering those issues.

6.2. Understanding the needs and expectations of interested parties.

The Company determines the interested parties that are relevant to the information security management system and the requirements related to these interested parties that are relevant to information security and include legal and contractual obligations.

6.3. Determining the scope of the information security management system

The scope of the Company's information security policy covers storage, access, and transfer of information during the Company's operations, through applications, systems, equipment, and the premises that create, process, transmit, host, or store information, whether in-house, personally owned or provided by external providers. The Company's information security policy applies to the staff, contractors, suppliers, and any party that has access to information transmitted during the Company's activities.

7. Risk Management

7.1. The Company considers the issues relevant to its business course, as well as the requirements of stakeholders, and determines the risks and opportunities that must be addressed, as follows:

- ✓ Ensuring that ISMS can achieve its intended outcomes.
- ✓ Preventing or reducing undesired effects.
- ✓ Achieving continual improvement.

7.2. The Company implements a plan to handle these risks and opportunities, integrate and implement its operations in its ISMS, and evaluate the effectiveness of these operations.

7.3. The Company performs periodic information security risk assessments, as well as when significant changes occur in the Company's processes and systems.

7.4. The Company keeps records of the results of the information security risk assessments.

7.5. The Company implements a program for handling information security risks and documents the results of handling information security risks.