**Standards for Information Security, Cyber Protection, and Business Continuity in the Israeli Payment Cards Ecosystem**

In recent years, we have seen significant developments in the payment card activity ecosystem in Israel. These developments have led to a dramatic increase in the number of participants in various stages of payment card transactions.

The SHVA (Payment Card Services) payment system operator, as well as other payment system participants, are supervised entities with high standards in the fields of information security, cyber protection, and business continuity. However, there are many participants in the ecosystem that are not supervised and have no obligation to meet any standards in these areas.

The activity of these participants exposes the Payment Card Services payment system to various risks in the areas of information security, cyber protection, and business continuity, and may impair the continuous functioning of payments using payment cards.

1. **Objective of this document**

In order to reduce these risks, it has become necessary to formulate standards for all participants in the ecosystem, including participants that are not subject to supervision or regulation. The standards presented in this document were formulated following consultation with the market, while balancing the need to enable the continued technological development of the Israeli payment card market and the need to ensure the proper functioning of payment cards in Israel, all while taking the needs of participants along the entire payment card transaction chain into account. This document details the broad agreements reached by the various participants all along the payment card transaction chain in the areas of information security, cyber protection, and business continuity.

1. **Applicability**
   1. The agreements reached in the market include uniform standards being met by all entities operating in the Israeli payment card ecosystem as follows:
      1. Check-out terminal manufacturers
      2. Software manufacturers
      3. Software providers
      4. Pin pad distributors
      5. CLP (closed loop payment) processors
      6. Payment aggregators
      7. Payment gateways
      8. Factoring companies
      9. Reconciliation companies
   2. This document will be validated and updated from time to time as needed and in accord with the requirements and agreements of the market.
2. **Minimum requirements for operating in the payment card ecosystem**
   1. Any entity operating in the Israeli payment card ecosystem and listed in the applicability section (hereinafter: “the participant”) will be required to declare before the system operator that it has technological abilities and resources, including the provision of the following documents:
      1. A valid Attestation of Completion (AOC) document confirming that it meets the PCI-DSS[[1]](#footnote-1) standard, on a yearly basis.
      2. Meeting the information security and cyber protection requirements listed in Section 4 of this document.
      3. Meeting the business continuity requirements listed in Section 5 of this document.
3. **Basic information security and cyber protection requirements** 
   1. **“Yuval” questionnaire** – Filling out the “Yuval” questionnaire self-declaration at least at the Basic Risk Level 1 (19 controls) and Authorization Level B, with regard to cyber protection and information security, once a year, including registration with the self-evaluation suppliers on the National Cyber Directorate website.[[2]](#footnote-2)
   2. **Information security supervisor** – The participant must appoint an information security supervisor with regard to information security and cyber protection, including responsibility for the implementation of the guidelines set out in this document.
   3. **Information protection and/or cyber protection policy** – It is the participant’s responsibility to ensure that it has an organizational infrastructure to support the containment and proper handling of an event such as the takeover of the management account, denial-of-service attacks (DDOS), vandalism, information leakage, and other threats.
   4. **Cyber and Finance Continuity Center** – The participant shall connect to the activity of the Cyber and Finance Continuity Center, and shall operate in conjunction with it, including: providing a contact person, cooperation with regard to suspicions and cyber events, realization and implementation of tools and services provided to it, and taking actions to reduce their effects providing feedback with regard to receipt of suspicious information and/or warnings from the Financial Cyber Center.
   5. **Robustness survey and penetration examinations** – The participant shall complete a robustness survey and examinations of penetrations to its information systems on a yearly basis, and this must include keeping and presenting documentation. If the survey or examination show negative findings, the participants must set out a plan for reducing them, and timetables for handling all the findings.
   6. **Log procedures and documentation** – The participant will be required to build a series of procedures to document logs and information having to do with payment card activity, maintain this information for at least two years, and present it when and as necessary.
   7. **Secure development** – The participant is responsible for maintaining development processes that are based on accepted secure development procedures. Insofar as developments are written and/or executed through a third party, the participant must ensure that they have undergone scanning and code standardization.
   8. **Protecting end-user stations and servers** – The participant must use accepted means to protect computers that are connected to the Internet, and perform regular security updates in the operating system. If security updates are required at high or critical levels, the participant must perform them immediately. In order to remove doubt, a check-out terminal is considered sensitive hardware, and should not be connected to the Internet, unless it is for the minimum required business needs for ongoing business activity. If Internet access is necessary, the participant must make sure that it is done through “secure surfing”.
   9. **Trustworthiness tests** – It is the participant’s responsibility to perform trustworthiness tests for all employees who will work directly with the system, including documentation of the tests and their presentation upon request.
   10. **Response to denial-of-service attacks (DDOS)** – If the participant outsources services for end points as part of its payment operations, it must provide a proper protection level against infrastructure-based and application-based denial-of-service attacks as part of the business continuity process of the payments system.
   11. **Authorizations** – The participant must make sure that employees are granted authorizations on a need-to-know basis. In addition, the participant must implement controls and documentation of the processes of end of employment, employee mobility, onboarding, and remote access, and must maintain the documentation of the authorizations and controls and present them upon request.
   12. **Employee awareness** – The participant shall carry out awareness training sessions for its employees with regard to information security, at least once a year, including the monitoring of attendance, and shall document the sessions and who has participated in them.
   13. **Drills** – The participant shall carry out periodic drills for employees and for the organization’s management.
4. **Basic business continuity requirements**
   1. **Business Continuity Officer** – The participant shall appoint a Business Continuity Officer to manage the issue, including responsibility for implementation of the guidelines contained in this document.
   2. **Threat identification process** – The participant shall identify threats that have the potential to expose its systems to risks and interruptions, and shall map critical processes for activity in the payments field and necessary resources (such as: peripheral systems, means, infrastructure, and so forth).
   3. **Business continuity plan** – The participant shall formulate a business continuity plan to ensure functional continuity under interruptions, including backup and recovery plans for its information systems that are connected to its activity in the payments field.
   4. **Incident reports** – In an emergency situation or in the case of an anomalous operational incident (including cyber), the participant shall report the details of the incident or emergency situation to the system operator up to two hours from the start of the incident. The participant must prepare an incident investigation up to seven business days following the start of the incident.
   5. **Infrastructure provider** – The participant shall ensure its ability to replace Internet infrastructure providers within a short time in the even that its Internet infrastructure provider experiences a failure. Participants that provide payment services to “existential services providers” such as food production facilities, gas stations, airports, emergency services, and so forth (hereinafter “existential services”) shall ensure their ability to automatically switch between two point-to-point (P2P) lines, each with a volume of 2MB, in the case of failure.
   6. **Service provider** – The participant shall ensure its ability to replace its Internet service provider within a short time in the case of a failure at its Internet service provider. Participants that provide payment services to existential services for the public shall ensure the ability to automatically switch between service providers in the event of a failure.
   7. **Communications backup** – The participant shall ensure its ability to perform an Internet or cellular backup of information and its ability to retrieve essential information in the case of a failure.
   8. **Bandwidth** – The participant shall define a bandwidth that shall take into account the volume of transactions and expected market changes, and shall maintain a bandwidth that shall be no less than 150 percent of its peak volume.
   9. **Monitoring and control** – The participant must regularly monitor the proper functioning of its communication lines and bandwidth.
   10. **Energy backup** – The participant shall prepare an energy backup for a case of electricity interruption (UPS, generation, and so forth).
   11. **Business continuity survey** – The participant shall, on a yearly basis, examine its preparedness to deal with business continuity events as detailed in this chapter.
   12. **Employee awareness** – The participant shall carry out awareness training sessions for its employees with regard to business continuity, at least once a year, including the monitoring of attendance, and shall document the sessions and who has participated in them.
   13. **Drills** – The participant shall carry out periodic drills for employees and for the organization’s management.
5. **Definitions**

* **Payment system operator** – The entity responsible for operating the payment system.

1. **Protocol organization** – The organization for managing the EMV terminal protocol in Israel.
2. **Payment card services system** – Operated by Automatic Bank Services Ltd. (SHVA).

* **Protocol** – A technological specification for a uniform and secure message structure developed in accordance with the unique needs and structure of the Israeli market, based on the protocol of the international schemes, which to serve to transfer approvals, transactions, and information between entities in the payment card transaction chain in Israel, in the segment between the terminal and the payment card payment system.
* **Cash register (checkout terminal) manufacturer** – An entity that develops or adjusts checkout service software for merchants, and includes managing debits and credits according to various means of payment, as well as inventory management, sales promotions, connection to the ERP systems, and more. The checkout software is connected via the communication protocol to the merchant’s terminal, and receives daily credit activity data from it.
* **POS terminal software manufacturer** – An entity that develops software for settling protocol-based payment card transactions.
* **POS terminal technology provider** – An entity that markets software to merchants from POS terminal software manufacturers.
* **Pin pad distributor** – An entity that provides software components that enable input and verification of PIN codes for payment cards when making an EMV transaction.
* **Closed loop payments processor** – A software company that provides payment services to private brand issuers such as consumer loyalty clubs, which enables payment and exercise of benefits in a “closed loop”.
* **Payment aggregator** – A company that coordinates merchants’ debits and credits made through payment cards under a settlement agreement with the merchant acquirer.
* **Payment gateway** – An entity that provides technological infrastructure to merchants in order to channel and process online trading transactions and is not involved in handling the settlement of the funds.
* **Factoring company** – An entity that provides merchants with services to advance credit payments (factoring) before the date of the expected receipt of the payment from the merchant acquirer.
* **Reconciliation Company** – An entity that provides merchants with reconciliation and control services between the debits and credits registered at the merchant and the consideration actually received for them from the merchant acquirer.
* **Internet infrastructure provider** – An entity that provides the physical infrastructure (fiber, servers, etc.) enabling connection to the Internet. **Internet service provider (ISP)** – An entity that provides customers with the availability and bandwidth to connect to the Internet
* **Business continuity plan (BCP)** – A written comprehensive work plan setting out the procedures and systems that are required in order to maintain business continuity or rehabilitate operations in case of emergency, interruptions, or failures.
* **Existential service providers** – As defined in the Emergency Labor Service Law, 5727–1967.
* **Cyber and Finance Continuity Center** – An operative center managed and led by the Ministry of Finance, to support the cyber defense of the financial system. The center is a main body coordinating between financial organizations and participants in Israel and entities in the national and international envelope. The center is responsible for coordinating activities to strengthen the resilience of the Israeli financial system and providing services and technologies to share defensive information with financial organizations and regulators. The center is located within the national Cyber Emergency Response Team (CERT), and operates in conjunction with the National Cyber Directorate.

1. **Revisions**

This document will be updated from time to time in accordance with changes and developments in the field.

|  |  |
| --- | --- |
| **Publication date** | **Details** |
| November 14, 2023 | Original publication |

1. Payment Card Industry Data Security Standard. [↑](#footnote-ref-1)
2. Explanation on the National Cyber Directorate’s “Yuval” questionnaire, and the questionnaire file in Excel, (in Hebrew) can be found at <https://www.gov.il/he/departments/news/querysupply> [↑](#footnote-ref-2)