INFORMATION TECHNOLOGY MANAGEMENT
CONTENTS

CHAPTER A	**GENERAL**	**357-3**
	1. Introduction	357-3
	2. Applicability	357-3
CHAPTER B	**SUPERVISION AND MANAGEMENT**	**357-4**
	3. Board of Directors	357-4
	4. Management	357-4
	5. Procedures	357-5
	6. Documentation, Record Keeping and Monitoring	357-5
	7. Internal Audit	357-6
CHAPTER C	**RISKS**	**357-7**
	8. Risk Assessment	357-7
CHAPTER D	**INFORMATION SECURITY**	**357-8**
	9. Information Security Manager	357-8
	10. Information Security	357-8
	11. Security Survey and Controlled Penetration Tests	357-9
	12. Access Control	357-10
	13. Encryption	357-11
	14. The Banking Corporation's Connection to the Internet	357-12
CHAPTER E	**BACKUP AND RECOVERY**	**357-14**
	15. Discussion by Management	357-14
	16. Backup and Recovery Arrangements	357-14
CHAPTER F	**OUTSOURCING**	**357-16**
	17. Outsourcing	357-16
	18. Contractual Agreement	357-16
CHAPTER G	**ELECTRONIC BANKING SERVICES**	**357-18**
	19. Definitions	357-18
	20. Contractual Agreement to Provide E-banking Services	357-19
	21. Proper Disclosure	357-21
	22. Means of Identification and Authorizations	357-21
	23. Password Management	357-22
	24. Control Measures	357-23
	25. E-banking Transactions in Favour of a Third Party	357-24
	26. List of Beneficiaries	357-25

ONLY THE HEBREW VERSION IS BINDING

27. Electronic Mail 357-25
28. Account Aggregation 357-26

CHAPTER H MISCELLANEOUS 357-29
29. Foreign Bank 357-29
30. Operations Requiring Consent and Operations Requiring Reporting 357-29

CHAPTER A: GENERAL

Introduction

1. (a) The information technology system is a central component in the operation and proper management of a banking corporation, in view of the information and all its aspects and implications having a substantial impact on the banking corporation's stability and development.

(b) Due to these factors a banking corporation's management must attribute the appropriate importance, both in its managerial hierarchy and in the necessary financial resources and human resources, for the proper management of information technology system.

(c) Without prejudice to the generality of the aforegoing, this regulation that includes detailed and general guidance, has been determined.

(d) This regulation accords with the principles for e-banking published by the International Committee on Banking Supervision (Basel Committee) in July 2003.

Applicability

2. This regulation shall apply to banking corporations and also to corporations as provided in sections 11(a)(3a) to (3c) and 11(b) of the Banking (Licensing) Law, 5741-1981 that were incorporated in Israel (hereinafter, a banking corporation).

CHAPTER B: SUPERVISION AND MANAGEMENT

Board of Directors

3. (a) A banking corporation's board of directors shall hold a periodic discussion and determine the banking corporation's information technology management policy pursuant to the provisions of section 6(n) of Proper Conduct of Banking Business Regulation No. 301 (Board of Directors).

(b) The information technology management policy shall *inter alia* include reference to:

(1) Information security;

(2) Backup and recovery principles in situations of malfunctions and disasters;

(3) Outsourcing;

(4) Development policy, including by end users;

(5) Use of new technologies in the context of e-banking.

Management

4. (a) A banking corporation's management shall appoint one manager, either a management member or a direct subordinate to the general manager, who shall bear responsibility for the entire information technology issues. The said manager shall have appropriate professional training and proven experience in the information technology field and the management thereof.

(b) A banking corporation's management shall appoint an information security manager, as set forth in section 9.

(c) A banking corporation's management shall hold an annual discussion on the implementation of the information technology management policy and the budgeting thereof and shall make the required decisions, while distinguishing between short-term relevant subjects and long-term relevant subjects.

(d) A banking corporation's management shall devote an annual discussion to the implementation of the information security policy with all its aspects.

(e) In determining the organisational structure of the unit charged with information technology management in the banking corporation, and in the definition of the

functions of the employees of this unit, the banking corporation's management shall maintain proper segregation of duties and authorities.

(f) A banking corporation's management shall define the types of operations and events in respect whereof warning must be given to management and other authorized bodies, including those that require a warning in real time.

Procedures

5. A banking corporation shall determine detailed procedures for every stage and for every process that deals with the management, operation, security, backup, continuity and control of information technology and shall carry out appropriate control of the performance thereof. These procedures shall be revised on an ongoing basis in accordance with the changes that occur in the relevant business environment and also in the technological environment.

Documentation, Record Keeping and Monitoring

6. (a) A banking corporation shall keep appropriate and current documentation for its information technology system.

(b) (1) A banking corporation shall maintain an audit trail that shall be based upon computerized recording (log) of access and transactions and queries performed in the banking corporation's information systems that shall *inter alia* include the identity of the access authorised person, the place, time and also particulars of the access subject.

(2) Notwithstanding the provisions of section (1) above, with regard to queries of the banking corporation's employees, the banking corporation shall maintain an audit trail, at its discretion, based on the risk assessment.

(3) A banking corporation shall determine the period of time for retaining the records as provided in section (1), provided that the period of time for retaining the records shall not be less than 60 days for queries records and 6 months for transactions records.

(c) A banking corporation shall inform its customers and its employees of the existence of retention processes of their activities.

(d) Subject to the provisions of section 4(f), the records management systems shall give warnings to the designated entities of unauthorised external activities and also of exceptional activities by the various types of users.

Internal Audit

7. (a) A banking corporation shall include within the context of its internal audit, an organisational unit for auditing its information technology. The person responsible for the internal audit in the information technology field shall have relevant professional training and experience to carry out the audit in this field.

(b) A banking corporation shall provide the internal audit with the tools required to carry out auditing and control in the information technology environment.

(c) In any event in which internal audit outsourcing is used in the information technology field, the assessment ability of the banking corporation's internal audit must be preserved.

CHAPTER C: RISKS

Risk Assessment

8. (a) A banking corporation's management shall perform a risk assessment of the information technology system. The risk assessment must address all the potential risks connected with managing the information technology system, such as:

- The banking corporation's internal and external system users;
- The system's environment;
- The system's operation and its implications on the corporation's business;
- The sensitivity of the information;
- Outsourcing.

(b) The risk assessment process shall be ongoing and the risk assessment shall be revised in accordance with changes in the various risk factors.

(c) The banking corporation shall, in accordance with the risk assessment, take the necessary measures to minimize the possibility of impairment to the information technology system and all its parts and to minimize potential damage.

CHAPTER D: INFORMATION SECURITY

Information Security Manager

9. (a) (1) The information security manager shall be subordinate to a member of the banking corporation's management.

(2) The information security manager shall not engage in functions that may create a conflict of interests, and in such regard he shall not be the information technology manager.

(3) A banking corporation's management shall determine the information security manager's fields of responsibility and the subjects decisions in respect whereof require his consideration. The fields of his responsibility shall *inter alia* include:

- Overall responsibility for the implementation of the information security policy in the banking corporation;
- Development and monitoring of the implementation of the information security plans in the banking corporation and examination of the effectiveness of the information security system;
- Dealing with exceptional information security events.

(4) A banking corporation shall provide the information security manager with the resources required for the performance of his duties.

(b) An information security manager shall have relevant professional training and experience in the field.

Information Security

10. (a) A banking corporation's management shall coordinate the information security principles in a document that shall be brought for the board of directors' approval. This document shall be revised periodically.

(b) A banking corporation shall implement security means - physical and logical, for the prevention, detection, rectification and documentation of exposures in the information technology system and the reporting thereof, in accordance with the risk assessment and also addressing the following aspects:

(1) Identification and authentication;

(2) Privacy;

(3) Integrity;

(4) Non-repudiation.

(c) A banking corporation shall routinely monitor the technological developments and adapt the security level and the control of access to its systems in accordance with changes in the risks level that emanates from such technological changes.

(d) A banking corporation shall act to separate the production environment from the development and test environment.

Security Survey and Controlled Penetration Tests

11. (a) (1) Periodically, in accordance with the risk assessment, the information security manager shall initiate a security survey of the banking corporation's information technology (hereinafter, the survey). The survey that shall be carried out shall assess the effectiveness of the protection means, having regard to the risk assessment, and ways of rectifying deficiencies that will be found shall be proposed.

(2) With regard to systems that were defined by the banking corporation as being of high risk, including e-banking systems, a survey must be carried out in the format set forth in section (1) above prior to implementing significant changes in such systems, when significant changes occur in the technological environment in which the systems operate, and also in anticipation of new systems as aforesaid being put into use, and at least once every 18 months.

(3) The survey's results shall include a detailed report of the findings and recommendations and a management summary that shall present the principal aspects thereof.

(b) The information security manager shall initiate controlled penetration tests into the banking corporation's information technology system to examine its resistance to internal and external risks. This operation shall be carried out at a frequency that accords with the various systems' specific risks, in accordance with the risk assessment.

(c) (1) The security survey and the controlled penetration tests as aforesaid shall be carried out by professional and independent entities, who are not part of the banking corporation, while avoiding conflicts of interests and taking the obliged cautionary measures.

(2) A banking corporation's management shall complete its discussions on the findings of the security survey and the controlled penetration tests and the implications thereof and shall make the necessary decisions, including determining a timetable for the implementation thereof, within a reasonable period of time after the time of the commencement thereof.

(d) Substantial findings that arose in the security survey and the controlled penetration tests shall be brought to the knowledge of the board of directors or an appropriate board of directors' committee.

Access Control

12. (a) (1) A banking corporation shall perform a unique personal identification of every entity with access to an information system (hereinafter, access authorised person) as a condition precedent for granting the access.

(2) Notwithstanding the provisions of section (1) above, in exceptional situations of suppliers and employees in respect whereof it is not possible to effect the aforegoing, the banking corporation shall apply appropriate alternative measures.

(b) (1) A banking corporation shall determine rules and tools for the identification of and the grant of authorizations to various entities for access to components of the information technology. These rules shall take into account the risk levels derived from the range of the user's responsibility and authority (according to a classification into groups), from the application itself, the sensitivity of the information and other information technology components.

(2) The classification into users' groups shall relate to the internal entities in the banking corporation and to the external entities (including customers, suppliers, etc.).

(3) A banking corporation shall put into operation tools for the management and control of the authorizations system.

(4) The means of access control to the information systems shall be with accepted techniques in such regard.

(c) (1) For the purposes of controlling access to information systems that were assessed as having a high risk, and in every case of remote access to the banking corporation's information technology by employees, suppliers and service providers, the banking corporation shall use a technology that combines identification and authentication of the user, privacy and integrity of the data and non-repudiation.

(2) Notwithstanding the provisions of section (1) above, a banking corporation is entitled to use alternative technology in the following events:

- In high risk systems other than via remote access, at the banking corporation's discretion, that shall be documented;
- In remote access by suppliers and service providers, where the use of technology as aforesaid is not possible for reasons that do not depend on the banking corporation.

(d) A banking corporation shall determine criteria for operating a time-out mechanism after a period of time in which there was no activity by the access authorised person. The period of time shall be determined with regard to the risk assessment.

Encryption

13. A banking corporation shall examine the need for encrypting data, including over the communications link, and in systems that were defined in the risks assessment as being of a high risk, provided that there shall be encryption in the following cases:

(a) E-banking via the Internet;

(b) Remote access to the banking corporation's computer, subject to the provisions of section 12(c);

(c) Access authorised persons' passwords.

The Banking Corporation's Connection to the Internet

14. (a) A banking corporation shall take measures to locate imitations of its Internet website and shall provide the customer with appropriate tools to ascertain the identity of the banking corporation's website.

(b) The banking corporation's connection to the Internet shall only be effected in the following cases:

(1) Employees' connection to the Internet, as detailed in subsections (c) and (d);

(2) Providing e-banking services, as detailed in Chapter G;

(3) Other use approved in advance by the Supervisor, as provided in section 30(a).

(c) A banking corporation's management shall determine the uses permitted for the banking corporation's employees connection to the Internet, subject to the provisions of subsection (d).

(d) The banking corporation's employees' connection to the Internet from work stations shall be permitted upon the fulfilment of one of the following:

(1) The work station is connected only to the Internet or to a network that is connected only to the Internet (stand alone) and there are no banking applications or sensitive information therein;

(2) The connection to the Internet shall be effected via a separate server of the banking corporation and shall be routinely controlled by the means set forth in subsection (e). In this configuration, connection to the Internet shall be effected for purposes of surfing and electronic mail only, without downloading files.

(3) Notwithstanding the provisions of section (2) above, a banking corporation that maintains full segregation between the banking corporation's network and the Internet, may permit the downloading of files while taking appropriate control measures.

(e) Pursuant to the provisions of section 10(c), the connection of the banking corporation's network to the Internet shall be secured at least by an antivirus, content-filtering, Intrusion Detection Systems (IDS) and a firewall.

(f) The banking corporation shall, in accordance with the risk assessment, apply computerized means for application control and scanning for weaknesses of the system.

CHAPTER E: BACKUP AND RECOVERY

Discussion by Management

15. (a) From time to time a banking corporation's management shall hold a discussion on the backup and recovery principles and shall make decisions in this area, with detailed reference to the risk assessment and the following matters:

(1) Definition of malfunction situations (including at the banking corporation's suppliers) and disasters (including natural disasters, fires, war and emergency) for all the organizational units and the implications thereof on the banking corporation's continued operations;

(2) Determining the vital business processes in situations of malfunctions and disasters, the relevant information systems for the operation thereof and the mode of such system's operation in situations as aforesaid;

(3) The various software, hardware and communications components;

(4) Aspects of the backup and recovery, including reference to routine backup, backup duration, backup frequency, backup media, maximum down times and the process of returning to routine work;

(5) Reliance on external entities at the time of interruptions to the normal operation of the information systems and the recovery time required by the banking corporation to return the information systems to normal operation.

(b) Within the context of the discussion, a decision shall be made as to the routine backup arrangements (including manpower and documentation backup) and investments in backup facilities and in other backup arrangements for significant systems that were determined in accordance with the provisions of subsection (a)(2) above.

Backup and Recovery Arrangements

16. (a) (1) A banking corporation shall maintain a detailed plan for operating its information technology in cases of malfunctions and disasters (hereinafter, disaster recovery plan), as provided in section 15.

(2) A banking corporation shall examine and revise the disaster recovery plan in accordance with the changes that have occurred in the period

that elapsed since the previous revision (including changes in the emergency provisions and in the risk assessment) at least once every two years and also at the time of effecting a significant change.

(b) At least once every two years and also at the time of effecting a significant change in the emergency provisions, a banking corporation shall test all its backup and recovery arrangements.

(c) The storage of backup equipment, vital software and information shall be at a location that is distant from the original storage location, so that events such as a natural disaster, war and the like shall not simultaneously damage the original equipment, software and information and backup and shall not prevent the use thereof.

(d) A banking corporation shall take measures that shall ensure the possibility of reconstructing information from backup copies, including information retained in means that are no longer being used.

CHAPTER F: OUTSOURCING

Outsourcing

17. (a) A banking corporation may effect the management, processing and storage activities of its information operations or the systems development, including consultancy services, know-how and other services, through entities outside the banking corporation (hereinafter, external entities).

(b) Notwithstanding the provisions of subsection (a), outsourcing as detailed below requires the Supervisor's consent, as provided in section 30(a):

(1) Outsourcing of core systems;

(2) Storage of information of whatsoever type with regard to the banking corporation's customers in systems that are not under its exclusive control;

(3) This clause does not apply to outsourcing services that a banking corporation receives as provided in section 11(a) of the Banking (Licensing) Law, 5741-1981, from the banking corporation that controls it or from an auxiliary corporation controlled by the banking corporation that controls it.

(c) Account aggregation services may not be outsourced.

(d) With respect to significant outsourcing, a banking corporation shall ascertain the service provider's reliability and economic viability and shall examine in advance the suitability of his qualifications and ability to perform the assignments.

Contractual Agreement

18. (a) The contract for the purposes of outsourcing shall be effected in a written agreement.

(b) With respect to significant outsourcing, the contractual agreement shall expressly relate to the following subjects at least:

(1) Definition of fields of responsibility of each of the parties to the agreement, including sub-contractors;

(2) Service level agreement (SLA);

(3) The duty of confidentiality, information security and emergency situations;

(4) Arrangements for the termination of the agreement and for resolving disputes. In such context the agreement shall also relate to arrangements that shall enable the banking corporation to operate and maintain the outsourcing activity in situations in which the external entity ceases providing the service (for example, by a source code being held by a trustee);

(5) The external entities' activities for the banking corporation may be audited on its behalf.

(c) The provisions of this section do not diminish from the banking corporation's responsibility for any activity effected on its behalf by external entities.

CHAPTER G: ELECTRONIC BANKING SERVICES

Definitions

19. (a) "**E-banking**" - Retrieval of information as to accounts of a customer of the banking corporation or executing transactions or giving instructions to execute transactions initiated by the banking corporation's customer via communications systems that are connected to the banking corporation's computer and that use a communications network (such as: telephony, Internet, cellular) or a combination between communications networks, save for transactions to which Proper Conduct of Banking Business Regulation No. 435 (Telephone Instructions) applies.

(b) (1) The service level of e-banking services are defined as follows:

(a) "**Service level (1)**" - Transferral of information from the banking corporation to the customer as to his accounts (transactions and balances);

(b) "**Service level (2)**" - Transactions and activities in the customer's accounts at the banking corporation (such as: transfer to fixed deposits, purchase of securities, transfer from account to account, ordering check books and the like);

(c) "**Service level (3)**" - Transactions for the benefit of accounts determined in advance by the customer by way of a list of beneficiaries;

(d) "**Service level (4)**" - Transactions for the benefit of accounts that are not included in one of the above service levels.

It is hereby clarified that each service level in sections (b) to (d) above includes the service levels that preceded it.

(2) An update of a customer's personal particulars is not included in service levels of e-banking services.

Contractual Agreement to Provide E-banking Services

20. (a) The contractual agreement between the banking corporation and the customer for the provision of e-banking services shall be signed at the branch, and shall allow the customer to select separately each service level and each communications channel that is offered by the banking corporation that the customer wishes to receive. At the time of signing the contractual agreement the customer shall be given initial identification means for the purposes of connecting to e-banking services.

(b) Notwithstanding the provisions of subsection (a) above, a contractual agreement may be made via communications channel (hereinafter, online agreement), provided that the following terms and conditions are fulfilled in respect thereof:

(1) Such agreement shall only enable services at service level (1), including account aggregation (as provided in section 28);

(2) A credit card company may, in addition to the provisions of section (1) above, also include the grant of credit in an online agreement, provided that the credit shall not exceed the customer's unutilised credit line;

(3) The agreement shall relate to only one communications channel;

(4) The wording of the agreement shall be shown in full on the screen in a clear and legible manner and it shall be possible to print it. The terms and conditions of the agreement shall not contradict the provisions of any other agreement that the customer signed, save for a previous online agreement;

(5) Notice of making an online agreement shall be sent to the customer by mail no later than seven days of the date of making the agreement, to the address recorded with the banking corporation;

(6) The identification of the customer for the purposes of the online agreement shall be based on at least two identification items that are not generally kept together;

(7) A banking corporation shall give the first identification means (such as: the user's code) and the initial password, to a customer who has not yet been given these items for the purposes of receiving e-banking services, at the branch or in two different ways (such as: one by mail, to the address recorded at the banking corporation, and the second via the Internet);

(8) The aforegoing in this section does not diminish from the provisions of the Banking (Service to Customer) (Proper Disclosure and Delivery of Documents) Rules, 5752-1992 (hereinafter, Proper Disclosure Rules).

(c) Notwithstanding the provisions of sections (b)(1), (b)(6) and (b)(7) above, a banking corporation may make an online agreement for any service level, provided that the following terms and conditions are fulfilled:

(1) The customer previously signed at the branch, up to three years prior to signing the online agreement, an agreement for the provision of e-banking services in another channel;

(2) The service level that the customer is joining shall not be extended beyond the existing service level that the customer joined in the past.

(3) The signing of an online agreement shall be done in the same channel that the customer joined in the past at the branch and with the same identification means.

(4) The channel that the customer joined in the past and through which the online agreement was signed, is not an automated teller machine (ATM) or service terminal.

(d) A banking corporation shall give written notice to the Supervisor of every new channel that can be obtained through an online agreement as provided in subsections (b) and (c) above.

ONLY THE HEBREW VERSION IS BINDING

(e) A banking corporation shall not offer e-banking services to customers with methods or means that are intended to prevent the customer receiving similar services from other banking corporations or service and information providers.

Proper Disclosure

21. A banking corporation shall present to its customers the conditions, exceptions and risks relating to using the e-banking services that it provides, shall bring to its customers' attention the security principles that it adopts in order to minimize such risks and shall recommend to its customers modes of protection against such risks. Furthermore, the banking corporation shall inform its customers that the aforegoing does not diminish from the responsibility of either of the parties.

Means of Identification and Authorizations

22. (a) Pursuant to the provisions of section 12(a), a banking corporation shall determine personal identification means for every customer who has account access authorization.

(b) In addition to the provisions of section (a) above, identification at ATMs and service terminals shall be done with at least two of the following three items:

(1) Something you know item;

(2) Something you have item;

(3) Something you are item.

Where the identification is made via identification means as provided in section (2) above, the banking corporation must apply a technology that shall, insofar as possible, prevent the possibility of unauthorised entities reconstructing the data contained in the item.

(c) A customer's authorizations to execute operations and retrieve information within the context of e-banking services shall not exceed the authorizations that the customer has in the account.

Password Management

23. (a) In managing passwords for the identification and authentication of its customers, a banking corporation shall take into account the service level and the risk level of the system.

(b) (1) The initial password shall be given to the customer personally with it being confidential.

(2) The initial password shall be given to the customer at the branch or via another communications channel which the customer joined prior thereto.

(3) For the purposes of this section, "initial password" includes a password given to a customer at the time of releasing a blocked password.

(4) The provisions of section (2) shall not apply to an online agreement as provided in section 20(b).

(c) A banking corporation shall initiate the replacement of the password by the customer in the following cases:

(1) Immediately after the first connection, with the initial password;

(2) In accordance with the service level and the risk level of the system, and at least once every six months.

(d) A banking corporation shall cancel the password (hereinafter, a blocked password) that was given to a customer in the following cases:

(1) The initial password, as provided in section (b), was not operated within 30 days from the issue thereof;

(2) At the customer's request or where the banking corporation suspects that unauthorized use was made of the password;

(3) After a certain number (that shall be determined by the banking corporation) of failed entry attempts, which shall in any event not exceed five consecutive failed attempts;

(4) After a period of six months of not using the specific system to which the password was attributed.

(e) Notwithstanding the provisions of subsection (b)(2), a banking corporation may release a blocked password with other means, provided that it shall also identify

the customer, in addition to the usual identification particulars according to specific identification particulars that were given by him in advance for such purpose, at the time of signing the agreement with the bank or according to particulars (that were not updated electronically) that are recorded with the banking corporation. In any event, the provisions of subsection (b)(1) above shall be complied with.

This arrangement shall not apply to an initial password that was not operated as provided in subsection (d)(1).

(f) The provisions of sections (c), (d)(1), (d)(4) and (e) shall not apply to e-banking services that use identification means as provided in section 22(b).

Control Measures

24. (a) In every entry by the customer to his account via e-banking services there shall be displayed for him, insofar as possible, details as to the time of his previous connection in the same channel.

(b) A banking corporation shall maintain a process of approving the customer for executing a transaction in an account that shall relate to the principal components of the transaction (type, nature, amount and the like). The customer must be enabled, insofar as possible, to save/print in real time all the particulars of the instruction that was actually given.

(c) A banking corporation shall take measures that are under its control to protect a computer/other instrument that the customer uses for communications against unauthorized use and the exposure of information as to the customer's account (such as: preventing saving the password in a browser, preventing saving Internet pages in "cache" memory and the like).

E-banking Transactions in Favour of a Third Party

25. (a) Online transactions in favour of a third party shall be executed in one of the following ways:

(1) Transactions to the credit of accounts defined in a list of beneficiaries as provided in section 26 below (service level (3)), with ceilings that shall be determined by the banking corporation and/or the customer;

(2) Transactions to the credit of other accounts (service level (4)) with the ceilings specified in subsection (c) below.

(b) (1) At the time of giving the instruction the customer shall be requested to specify the recipient's particulars and the nature of the payment.

(2) A banking corporation shall transmit data as to the payer's particulars and, insofar as possible, the nature of the payment, so that it shall be possible to clearly present them in the beneficiary's account summary.

(c) Ceilings for transactions to the credit of other accounts (service level (4)) -

A banking corporation shall determine a ceiling for the single payment and for the total payments being made from the account during the course of one month according to the type of the customer, provided that it shall not exceed the following ceilings:

(1) In the business sector - a single payment ceiling shall not exceed NIS 200,000 and the total payments made from the account during the period of one month shall not exceed NIS 1,000,000;

(2) In the private sector - a single payment ceiling shall not exceed NIS 6,000 and the total payments made from the account during the period of one month shall not exceed NIS 50,000.

(d) Notwithstanding the provisions of subsection (a) above, a banking corporation is entitled to execute transactions to the credit of other beneficiaries (service level (4)) with technology as provided in section 12(c)(1) at the single transaction level with ceilings that shall be determined by the banking corporation and/or the customer.

List of Beneficiaries

26. (a) A banking corporation shall maintain a computerized list of beneficiaries for every customer wishing to receive the service. The list of beneficiaries shall be approved in writing and in advance by the customer at the branch.

(b) The customer shall be entitled to send the banking corporation revisions to the list of beneficiaries at the branch or electronically, provided that the validity of making a revision electronically shall be conditional upon using technology as provided in section 12(c)(1).

(c) (1) A customer shall be required at least once a year to confirm the list of beneficiaries and all its particulars, including the ceiling for payment of each beneficiary included in the list, if any. In the request to confirm the list of beneficiaries the banking corporation shall specify the implications of failing to confirm the list in time, as specified in section (d) below.

(2) The confirmation can be made in writing at the branch or by sending a letter to the customer's address that shall be confirmed (or amended) by the customer by signing it and returning it by mail, or electronically using technology as provided in section 12(c)(1).

(d) A list that is not confirmed by the customer within 45 days of the banking corporation's request - shall expire. The banking corporation must to inform the customer of such request at the time of his signing the list of beneficiaries as provided in subsection (a) above.

Electronic Mail

27. (a) A banking corporation's management shall determine the uses and types of activities that the banking corporation's customers are permitted to execute via electronic mail.

(b) A banking corporation shall take into account the degree of the need for unequivocal identification of a customer sending electronic mail, authentication and security of the contents of the message, maintaining confidentiality of the

information and non-repudiation and in accordance with the types of activities as provided in subsection (a).

(c) Notwithstanding the provisions of subsections (a) and (b) above, the giving of instructions to execute operations of the banking corporation's customers (hereinafter, execution instructions) by electronic mail shall be given using technologies as provided in section 12(c)(1).

(d) A banking corporation may send by electronic mail or via the corporation's website notices that the Proper Disclosure Rules permit to be sent to a customer by mail as well as other information to which the confidentiality duty applies, provided that the following terms and conditions are fulfilled:

(1) The customer signs an agreement as provided in section 20;

(2) The customer can terminate such service at any time, at his request;

(3) The banking corporation operates computerized tools that enable it to unequivocally determine whether the customer received and opened the mail or downloaded the mail message to his personal computer or printed it. The banking corporation shall also retain the required operating information for the examination and management of monitoring of compliance with the Proper Disclosure Rules;

(4) The transmission of the mail from the bank to the customer shall be in a secure environment, while taking appropriate measures to maintain confidentiality of the information.

Account Aggregation

28. (a) A banking corporation may offer its customers and customers of other banking corporations an "account aggregation" service (hereinafter, the service) with a "user driven" model (such as software in the customer's computer) or a "third party" model (such as via the banking corporation's server).

(b) A banking corporation that offers the service with the "third party" model shall do so via a designated server of the corporation that is only intended for the said service.

(c) The service shall be provided by the banking corporation upon the following terms and conditions:

(1) The service is limited only to aggregation of information;

(2) The banking corporation and its employees shall not have access to the customers' information that is received from other banking corporations (hereinafter, the customers' information) and they shall not use it. For such purpose, the banking corporation shall apply technological solutions that shall support the confidentiality and protection of the information that other banking corporations transmit as to their customers and it shall provide an audit trail for attempts to access the information, including the information as to the means of access to the other corporations' accounts;

(3) Notwithstanding the provisions of sections (1) and (2), a banking corporation may itself only use the customer's aggregate (the total) information provided that it received express approval from the customer to do so and that the information shall be sent for the customer's knowledge only;

(4) A banking corporation shall only operate the service on the customer's initiation and at the time of the request;

(5) A banking corporation providing the service shall not accumulate the customers' information over time, but shall delete it at or about the time of the transmission thereof to the customer;

(6) A banking corporation providing the service shall not enable the replacement of other banking corporations' passwords via an account aggregation system;

(7) (a) A banking corporation shall delete from the relevant data bases all the personal information and the information that enables access to accounts of a customer wishing to be disconnected from the service;

(b) The continued retention of personal particulars of users who are not customers of the bank and were disconnected from the service is conditional upon receiving specific approval therefor at the time of joining the service;

(8) A banking corporation shall not make the provision of the service conditional upon the customer's consent to the provisions of sections (3) and (7)(b) above.

(d) A banking corporation wishing to provide account aggregation services shall apply for a permit for such purpose from the Supervisor of Banks, as provided in section 30(a).

CHAPTER H: MISCELLANEOUS

Foreign Bank

29. The regulation shall apply *verbatim* to a foreign bank, save for the changes set forth below:

(a) Throughout the regulation the expression "information technology system" shall be replaced by the expression "the local information technology system, including the interfaces of such system with the overseas bank's system".

(b) Section 3 shall apply to the management in lieu of the board of directors.

(c) The following sentence shall be added to subsection 11(a)(3):
"A copy of the managerial summary shall be sent for the knowledge of the person responsible for the information security at the parent bank".

(d) The following section shall be added to section 16 of the regulation:
"(e) A foreign bank shall at all times retain in the local information systems at its branches in Israel full data containing all the personal and administrative particulars as to the owners of the accounts, the legal representatives and the signatory rights and also all the current balances of the accounts being conducted at its branches in Israel."

(e) The sections specified below can be effected by the parent bank and not directly by the foreign bank, provided that the foreign bank shall, if necessary, also make the necessary adaptations to comply *verbatim* with the following sections of the regulation: 5, 6(a), 6(b), 7, 8(a), 10(a), 10(b), 12, 13, 14, 16(d), 21, 22, 23, 24, 25, 26, 27(c), 27(d)(3), 27(d)(4) and 28.

(f) In exceptional cases, a foreign bank that believes that certain sections of this regulation are not applicable to it, may apply to the Supervisor in order to adapt the applicability thereof and/or the mode of the application in respect of it, as provided in section 30(a).

Operations Requiring Consent and Operations Requiring Reporting

30. (a) A banking corporation wishing to perform one of the following operations shall give prior notice to the Supervisor. If the Supervisor does not notify the

banking corporation of non-approval of the operations within 90 days, the banking corporation can deem such to be approval:

(1) Use of new communications channels or new instruments for the purpose of e-banking that were not in use in the banking system in Israel;

(2) The banking corporation's connection to the Internet pursuant to section 14(b)(3);

(3) Outsourcing as provided in section 17(b);

(4) Offering an account aggregation service as provided in section 28(d);

(5) Adapting the applicability of sections of the regulation for a foreign bank as provided in section 29(f).

(b) A banking corporation shall report the following subjects and events to the Supervisor of Banks:

(1) Exceptional events, including significant penetration and attack attempts, actual penetrations into computer systems, a crash of central systems, operation of the banking corporation's emergency plan and the like;

(2) Discontinuation of significant services for customers in consequence of an unplanned shutdown of computerized systems' operations for a period of time of more than one business day;

(3) The establishment of an ancillary corporation that shall engage in the information technology field;

(4) A decision as to anticipated significant changes in the information technology management policy, material conversion of the computerized systems and re-computerisation of central systems and their like;

(5) A decision as to expanding the service level, a material change in the communications channels or a new initiative in providing e-banking services;

(6) Notice of "online agreement" (section 20(d)).

(c) Notices and reports pursuant to sections (a) and (b) above have to be sent to the Information and Reporting Unit at the Bank of Israel's Banking Supervision Department.

(d) Reports pursuant to sections (b)(1) and (b)(2) above have to be sent within one business day of the occurrence of the event the subject of the reports. Notices pursuant to sections (b)(3) to (b)(6) have to be sent 30 days in advance.

* * *