Riga, 26 September 2018

Regulations No 158
(Meeting of the Board of the Financial and Capital Market Commission
Min. No 44; paragraph 5)

Regulations on Information Systems Security

Issued in accordance with
Article 7, Paragraph one, Clause 1 of the Law on the Financial and Capital Market Commission,
Section 34.[1], Paragraph two and Section 50, Paragraph three of the Credit Institution Law,
Article 45, Paragraph one and Article104[1], Paragraph five of the Law on Payment Services and Electronic Money,
Article 123.[5], Paragraph two and Article 124, Paragraph 1.[1] of the Law on the Financial Instruments Market
and Section 28, Paragraph six of the Law on Private Pension Funds

I. General Provisions

1. Regulations on Information Systems Security (hereinafter – the Regulations) shall be binding on the participants of the financial and capital market registered in Latvia (hereinafter – market participant), namely, credit institutions, credit unions, payment institutions, electronic money institutions, insurance undertakings, insurance intermediaries, private pension funds, organizers of a regulated market, central securities depository, investment firms, investment management companies and alternative investment fund managers.

2. The purpose of the Regulations is to limit information systems (hereinafter also - IS) security risks when providing services to market participants and clients, in general aiming at a prudential management level of information systems risks (risk appetite), as well as prescribe uniform structured requirements for the management of market participant IS security risks.

3. A market participant in implementing additional safeguards shall observe the proportionality principle and risk-based approach taking into account the scope of activities, the number of employees, the type of services provided and their complexity as well as the level of information technology (hereinafter – IT) application.

II. Terms Used in the Regulations

4. Audit trail – trails available for analysis in which data about specific IS events is registered (access to data, as well as input, correction, deletion, output of data, etc.).

5. Security measures – technical and organisational measures within a risk management framework to reduce the IS risks to an acceptable level.

6. Vulnerability – IS deficiency that may result in exposing the IS to danger and likely impact on IS security.

7. Information system (IS) – data entry, storage and processing systems that ensure performance of functions and provide for an end-user's access to data or information stored in the IS.

8. Information confidentiality – ensuring access to information only by authorized persons or processes.

9. Information integrity – accuracy, correctness and completeness of information and processing methodology thereof.

10. Information availability – possibility for authorized persons to use the information at a specific time and place.

11. Information resources – information units that include data files containing information stored and processed in the information system and available to information system users, as well as all the information system input and output documents irrespective of the data medium used.

12. Data or information owner – a person who is responsible for information resources and disposes of them upon the assignment of a market participant.

13. Strong customer authentication – an authentication based on the use of two or more elements categorised as knowledge (something only the user knows, for example, a password, PIN), possession (something only the user possesses, for example, a particular code calculator, cell phone) and inherence (unique characteristics of the user, e.g., a finger print) that are independent, i.e. the breach of one element does not compromise the others, and that is designed in such a way as to protect the confidentiality of the authentication data.

14. IS security – ensuring the IS requirements for confidentiality, integrity and availability.

15. IS security incident – an event or a number of correlated events that a market participant has not planned and that have or may have an adverse impact on IS security.

16. IS end-user – a person who uses the IS within its authority.

17. Risk – potential inability of institution to fully and qualitatively perform any of its obligations or functions related to the IS functionality caused by potential undesirable event and combination of its consequences.

18. Technology resources – the IS component that includes the system software, application software, auxiliary software, system files, computers, computer networks, equipment and other devices that ensure operation of information system.

19. Technology resource owner – a person who is responsible for technology resources and disposes of them upon the assignment of a market participant.

III. IS Security Management

20. Management commitment and support

20.1. Management of a market participant shall be responsible for setting and implementing the IS policy and IT strategy, determining employees' duties and responsibilities, arranging control measures, as well as assigning appropriate resources for ensuring adequate IS security and IS audit functionality.

20.2. The purpose of IS security policy shall be to define the position of the management of a market participant and support for ensuring IS security in compliance with the needs of market participant and its clients.

21. Internal documentation

21.1. A market participant shall approve a set of hierarchically structured documentation that formulates the IS management, including the IS security management. Defining the IS security management, the IS security objectives shall be set as well as the roles, responsibility and application of IS security measures.

21.2. At least those IS management processes shall be documented, a failure of which may create the IS security risks.

21.3. A market participant shall ensure updating of internal documentation and their availability to the employees.

21.4. A market participant shall determine responsibility of employees for a failure to meet internal requirements.

21.5. A market participant shall create and maintain updated information flow scheme.

22. IS security or IS risk management function (hereinafter – IS security function)

22.1. A market participant shall ensure the IS security function to perform risk monitoring and implement the IS security measures.

22.2. Within the IS security function, a market participant shall ensure at least:

22.2.1. working out and updating of IS security documentation;

22.2.2. coordination of IS classification, threat identification and IS risk management processes;

22.2.3. notifying the management of compliance with requirements and of severe IS security incidents;

22.2.4. supervision over the security measures;

22.2.5. training employees and informing them on the IS security issues;

22.2.6. management of IS security incidents;

22.2.7. participation in planning recovery of IS operation and continuity.

22.4.3. A market participant shall ensure splitting functions into the IS security function and IS development and maintenance functions and the obligation to directly communicate the essential IS security events to the market participant management. If an employee responsible for the IS security performs double duties then the principle of distribution of duties shall be complied with, namely, the employee is forbidden from self-supervision.

23. IS audit function

23.1. A market participant shall ensure performance of IS audit function in order to provide for an independent examination of the IS security measures implementation.

23.2. Audit function may be performed also by outsourcing service provider.

24. Outsourced service management

24.1. A market participant may use services provided by a third party – an outsourcing service provider. A market participant shall carry out accounting of all the outsourced services used.

24.2. Using outsourced service shall not release a market participant from responsibilities prescribed by laws and regulations or agreement with its clients – it shall be responsible for the performance of the service provider to the same extent as for its own performance. The minimum level of IS security if the IS is developed or maintained by outsourcing service provider, shall not be lower than the level specified by a market participant.

24.3. Prior to making a decision on acquiring outsourced services a market participant shall evaluate providers, define requirements for service quality, security and availability, assess risks and specify strategy for service termination.

24.4. A market participant shall draw up and keep up-to-date a list all outsourced services and carry out supervision of outsourced services, monitoring their compliance with security and operational objectives. A contract between a market participant and outsourcing service provider shall include a requirement for outsourced service control, e.g. a clear description of service, security requirements, confidentiality obligations, the right to receive the necessary information for monitoring the service, requirement to outsourcing service providers to immediately report incidents, the right to terminate the outsourcing contract.

24.5. Using outsourcing, including cloud computing, a market participant shall have a duty to maintain the necessary control over information that contain data on the clients of market participant. Classified IS of market participant shall be physically and logically separated in a safe manner from the IS of other clients of outsourcing service provider. The plan of service termination shall be drawn up and regularly updated, providing for returning back data, software and technical resources and deletion of client information with the service provider.

24.6. A market participant shall perform supervision of outsourced service quality and security control, including reports on the service quality and incidents.

24.7. In provision of outsourced services to a third party using the IS, including an authentication outsourced service, a market participant shall have a duty to monitor the implementation of solution in a third party enterprise. A market participant shall notify business partners of the risks associated with the use of such services. In case of failure to meet security requirements cooperation shall be terminated.

IV. Management of IS Resources

25. Ownership of resources

25.1. A market participant shall in writing assign the IS resource owners (information and technological resources) for all information and technology resources.

25.2. Obligations of information resource owner shall be as follows:

25.2.1. to classify the information resources in its ownership;

25.2.2. to participate in risk analysis of the information resources in its ownership and approve it;

25.2.3. to authorize the IS access rights;

25.2.4. to approve changes in the IS;

25.2.5. to set requirements for audit trail;

25.2.6. to cooperate with the IS technology resource owner regarding the IS functionality and security issues.

25.3. A market participant shall ensure training of information resource owners regarding their obligations.

25.4. Obligations of technology resource holder shall be as follows:

25.4.1. to ensure measures of physical and logical security of technology resources;

25.4.2. to cooperate with the information resource owner in order to fulfil its requirements regarding the protection of information resources and access to them;

25.4.3. to participate in risk analysis, to identify the IS threats related to the technology resources and to evaluate the likelihood of threat materialisation;

25.4.4. to ensure the IS recovery procedures in case of technology resource damages and disturbed IS functions;

25.4.5. to cooperate with the IS information resource owner regarding the IS functionality and security issues.

25.5. A resource owner may assign resource custodians, namely, persons whose daily duties include relevant IS resources or their share, to fulfil the mentioned obligations.

26. IS and IT classification

26.1. A market participant shall draw up and keep up-to-date a list of IS or IT services on a regular basis and carry out their classification.

26.2. The purpose of classification shall be to evaluate importance of the IS and/or IT services and to ensure their protection according to importance of service and applicable operational and security risks. A market participant shall carry out the IS classification, indicating the level of confidentiality, value and availability.

26.3. A market participant shall regularly revaluate classification of IS and/or IT services.

26.4. Requirements for the use and protection of classified information according to the information classification level shall be set up by a market participant.

V. Risk Analysis and Management

27. A market participant shall regularly monitor threats and vulnerabilities and revise the risk scenarios that have an impact on the IS and/or IT services. IS risk management shall be integrated in the institution's overall risk management framework.

28. The purpose of risk analysis and management shall be as follows:

28.1. to set the acceptable risk level (risk limit or appetite);

28.2. to assess probability of vulnerability and threat to the IS under various scenarios;

28.3. to assess potential damage or impact that could be done to a market participant, customer or other person if the IS security is not ensured;

28.4. to set additional security measures if the risk is unacceptable;

28.5. to accept the risk remaining after the implementation of security measures (compliance with the set risk limit).

29. Risk analysis process shall be conducted on a regular basis. A market participant shall carry it out throughout the IS life cycle, i.e. launching the IS project, making fundamental changes in the IS, reviewing the IS classification, upon occurrence of essential threats or severe incidents, or their growing in number.

30. Risk analysis shall be performed using documented methodology that determines also risk analysis frequency. A market participant shall use such risk analysis methodology that allows efficiently implement objectives set in paragraph 28 thereof.

31. A market participant shall project and implement security measures if the risk is recognised as unacceptable during the risk analysis and set priorities, terms and responsible employees for the projected security measures.

32. The purpose of security measures shall be to reduce the remaining risk to an acceptable level. A market participant shall assign security measures based on the commensurability between the costs of security measures and potential loss.

VI. Role of Staff in IS Security

33. Within the framework of risk management, a market participant shall take measures that restrict the IS security risks ensuing from the activity or inactivity of employees, as well as shall determine the role of employees in applying the IS security measures and facilitate staff comprehension on the IS use procedure and safeguards necessity.

34. A market participant shall ensure compliance of IS end-users' competence with the needs of IS application.

35. A market participant shall instruct employees before assuming their duties regarding the IS regulatory documentation.

36. A market participant shall assign to the IS end-user following obligations and duties:
36.1. liability for failure to meet the IS regulatory requirements;
36.2. liability for the activities that have been carried out in the IS under the name of IS end-user;
36.3. adherence to confidentiality obligations regarding the data the person deals with in exercising his/her duties and obligations;
36.4. obligation to inform the relevant person (for instance, IS security manager) about IT security incidents and threats.

37. Enhancing security awareness
37.1. Regular planned activities shall be conducted aimed at the IS security awareness raising among individuals and overall staff.
37.2. A market participant shall determine frequency and procedures for informing and training of employees in the IS security matters.
37.3. Employees shall be trained in the classified information protection.

VII. Physical and Environmental Security Management

38. Within the framework of risk management a market participant shall carry out measures of IS physical security that protect from an undesirable environmental (fire, flood, temperature fluctuations, etc.), technical (inappropriate power supply, impact of electromagnetic field, etc.) and human factors (direct or indirect damages, theft, etc.).

39. Physical protection of IS infrastructure (technology resources, including servers, disc array, computer and cable network, etc., except for technology resources of end-users)
39.1. IS infrastructure shall be operated in restricted access premises, the physical security of which shall ensure access only to authorized persons. If required technically, when operating outside the restricted access area, the IS technology resources shall be physically isolated. The IS server room shall be located in the locations of the building with the smallest probability of threat materialisation.
39.2. A market participant shall determine the persons who may enter the server room mentioned in paragraph 41.1 of the Regulations and shall document their access into the list.

Only the persons who need a physical access to the IS infrastructure to fulfil their duties shall be included into the access list.

39.3. Third parties may stay in the IS server room only when attended by authorized persons.

39.4. A market participant shall ensure adequate climate control in the IS server room (humidity, temperature, etc.) in compliance with requirements set by the manufacturers of IS infrastructure operating equipment.

39.5. IS server room shall be equipped with security alarm system and environment detectors.

39.6. IT resource administrative staff work places shall be located in restricted access premises.

40. Physical protection of data media

40.1. A market participant shall take the necessary precautions to protect the physical media, depending on the IS classification, whatever their type (including the removed disc equipment, paper, flash cards, etc.).

40.2. A market participant shall set a procedure according to which the data media shall be used, stored and safely destroyed.

40.3. Within the framework of protection of data media, a market participant shall perform the physical protection of the data output devices, by preventing unauthorized use of information resources (for example, safeguarding of printing devices, restricting interface use).

40.4. If it is planned to destroy data media that contain classified IS information resources, then it shall be performed in a way to prevent from data recovery.

41. A market participant shall take additional physical protection measures depending on the IS classification level. In case of necessity physical protection measures may be compensated by logical security measures (software and processes).

VIII. Management of Information Systems Access Rights

42. Registration of a new user, as well as rights granting, blocking and cancellation procedures shall be carried out upon a documented request approved by the information resource owner. Documentation method shall enable effective control over the current access rights process.

43. A unique user code shall be assigned to each IS end-user and the IS administrator.

44. Determination of end-user's authenticity

44.1. The purpose for determining the authenticity of end-user shall be to make certain that the classified IS resources are used by the authorized owner of user code.

44.2. A market participant shall set a procedure for the use of authentication measures (for example, a password, codes calculator, private key, biometric measures, etc.) including password policy (password's length, complexity, validity and history).

44.3. The IS passwords shall be stored in an encrypted form. When entering a password it shall not be decipherable on the screen. A password shall be immediately changed if it could have become known to an unauthorized person.

44.4. Establishing, providing and activating authentication measure, a market participant shall ensure that it is available only to the relevant user code owner (including a safe process for establishing identification and user password).

44.5. If the technologies used allow, in addition to the built-in administrator account a market participant shall set up individual accounts for each administrator, which is used daily for the IS maintenance operations. Copies of IS administrator codes and passwords shall be stored in a safe and controlled mode outside the technological infrastructure.

45. A market participant shall determine access rights to the IS in accordance with the approved and documented roles or user profiles. The IS user shall be granted with access rights only to information and functions that are necessary to perform their duties (least privilege principle shall be applied).

46. In setting up individual accounts for IS administrators, in addition to the least privilege principle, methods shall be used to separate high-privilege accounts and limit their use to carrying out daily operations.

47. In setting up accounts for carrying out various technological processes, for example, a backup process, privileges granted to the account shall be limited to those needed to carry out daily operations.

48. In using high-privilege user accounts by the IS administrators, access to critical systems administration shall be safely separated from public network, for example, internet browsing environment.

49. In case of an IS user or administrator work duties change or termination of labour relations, the rights of IS user and administrator shall be immediately changed or blocked.

50. Examination of current access rights shall be carried out on a regular basis to monitor compliance with provisions laid down in paragraphs 45-49 of the Regulations.

IX. Communications and Operation Management

51. A market participant shall determine obligations and responsibilities for employees, who ensure the IS maintenance, providing for substitutability and maintenance of qualification. For controlling processes, the splitting of functions shall be ensured.

52. Configuration management and control

52.1. A market participant shall record technology resources and their existing configuration.

52.2. A market participant shall determine procedures for requesting, authorizing, testing, changing and documenting technology resources.

52.3. Within the framework of risk control, a market participant shall maintain and monitor the IS configuration taking into account hardening standards and identified IS vulnerability, as well as carry out configuration integrity checks.

52.4. Within the framework of risk control, a market participant shall carry out required and technologically possible changes in technology resource standard configuration and reduce functionality to the minimum required amount.

52.5. A market participant shall in due time maintain necessary updating and security patches of IS standard software.

53. Computer network security

53.1. Local and external computer networks shall be segregated. The data flow between the local computer network and external computer network shall allow only those services that are necessary for the fulfilment of market participant functions.

53.2. A market participant shall develop and maintain up-to-date computer network and access scheme.

53.3. A market participant shall regularly check existence of all external connections to verify that there are only those connections that meet the requirements essential for the market participant activities.

53.4. Within the framework of risk control, a market participant shall implement the required and possible additional restrictions on the data flow (including restrictions on application, sites) between the local computer network and external computer network.

53.5. A market participant shall carry out computer network monitoring and vulnerability control (including malicious programs).

53.6. In case the IS administration is performed from a remote location it shall be protected by using cryptography (for instance, virtual private network (VPN)) and strong authentication.

53.7. In case a wireless data transmission technology is used, additional protection shall be performed within the framework of risk management to ensure only authorized IS usage.

54. Protection of personal computers and equipment

54.1. A market participant shall determine information resources that may be stored in the individual data processing equipment and how they shall be protected, including desktop and portable computers (hereinafter – personal computer), smart phone, tablet PCs, etc.

54.2. Only the software and configuration shall be installed and used in the personal computer that is prescribed by a market participant, who also shall establish procedures and take measures to protect the computer against malicious programs using, for example, anti-virus software, software protection policy.

54.3. Functionality of a personal computer shall be limited to the level of functions necessary for work needs; a market participant shall control the use of computer ports and equipment connection, control access to public network information (blacklisting, white-listing) and logically separate access to the public network information from the internal IS using, for example, virtualization.

54.4. Personal computer shall be connected only to the computer network determined by a market participant.

54.5. A market participant shall ensure that when the user leaves a personal computer unattended, the IS use shall be continued or connection to computer network shall be possible only if the authentication of a user is performed.

54.6. Classified information shall be stored and transmitted encrypted when using the personal computers subject to increased physical security threats, including portable equipment, which is used outside market participant's business offices.

54.7. A market participant shall record all the personal computers available that may be used outside business premises to identify the persons who use relevant equipment.

54.8. In case employees are permitted to use their computers for work needs a market participant shall establish computer usage instructions. This procedure shall not reduce the set IS security level.

54.9. If a remote access to the market participant's IS is provided using a smart phone or tablet PC, security of those devices shall be protected in order to prevent coming of sensitive data of a client or a market participant into possession of third parties in the event of incident (e.g. protected access to a device, data are not stored in a device and automatically deleted after a session).

55. Data backup process

55.1. To limit integrity and availability risks, a market participant shall create a data backup.

55.2. Procedure for data backup copying shall be established and documented specifying technology and activities for creating a data backup and recovery of information, as well as frequency and amount of data backups in view of a tolerable period of time while the IS may probably be unavailable (recovery time objective), and a time period in which data might be lost (recovery point objective), as well as frequency for examination of copying and recovery procedures.

55.3. A market participant shall ensure that at least for those IS that provide material services for a market participant or its client, backup copying shall be performed by a risk minimising method (data storage devices physically or logically separated from the IS). Data backups shall be stored in a location that is geographically detached from the IS.

55.4. A market participant shall protect data backups against the unauthorized use and data corruption.

56. IS monitoring

56.1. For the IS monitoring, a market participant shall set at least following objectives: to take preventive measures for the IS security maintenance and timely identification of incidents. Supervisory activities shall be applied in compliance with the IS classification.

56.2. A market participant shall carry out the IS supervision on a regular basis by:

56.2.1. timely identifying both internal and external threats;

56.2.2. identifying and preventing the IS vulnerability;

56.2.3. supervising unauthorized use of equipment and software and preventing from it;

56.2.4. monitoring access to the systems by the IS administrators and recording the activities carried out;

56.2.5. controlling access to the IS by outsourcing service provider;

56.2.6. monitoring availability of IS, equipment and processes.

57. Audit trail management

57.1. To identify the users' activities and IS errors a market participant shall create, store and analyse audit trails.

57.2. Audit trails shall include at least the date and time of all successful and unsuccessful connections as well as the users' codes. Additional audit trails shall be performed on the change of IS parameters, including activities with users accounts as far as it can be ensured by technological solution.

57.3. A market participant shall use methods and tools that provide for an efficient analysis of audit trails. Those tools shall be available only to the authorized staff.

57.4. A market participant shall ensure integrity of audit trails.

57.5. A market participant shall synchronise time records of all IS that are interconnected to exchange data or process transactions.

58. Use of a cryptography method

58.1. Cryptography method shall be used by a market participant depending on the confidentiality level of information resources.

58.2. A market participant shall determine a procedure for the use of cryptography method, as well as ensure its protection.

X. Remote services security management

59. By offering remote services to clients a market participant shall ensure security management of services in order to minimise their client risks.

60. Client authentication tools (equipment, software) shall be required, provided and activated in a secure manner. A market participant shall carry out identification of client and other related activities to ensure that the remote service authentication tools are received only by its owner.

61. A payment service provider shall have a duty to apply strong client authentication where the client accesses a payment account online, initiates a payment, accesses or changes sensitive data, including the list of reliable beneficiaries, by using remote service.

62. Payment service providers may use alternative client authentication measures for:

62.1. payments to a reliable beneficiary included in the approved white list;

62.2. transactions between two accounts of a single same client, maintained by the same payment service provider;

62.3. transfers between the same payment service provider accounts if such option is provided under the risk assessment performed by the payment service provider;

62.4. payments of small amounts up to 30 euro, if the total amount of previous remote electronic payment transactions initiated by the payer since the previous application of strong authentication does not exceed 100 euro.

63. Payment cards issued by the payment service provider shall support card holder's strong authentication for online transactions.

64. Payment service providers shall apply transaction supervision and monitoring solutions intended to prevent, identify and block fraudulent payments before the payment service provider has authorised them. Specific monitoring and assessment processes shall be applied to suspicious and high-risk transactions.

65. A payment service provider shall establish limits for payments. A payment service provider and the client may agree on the payment limit for each payment instrument appropriate to the risk profile. An option to adjust the limits to the agreed ceiling of the limit shall be ensured for the payer.

66. Payment service providers shall ensure an option to be alerted about the initiated payments and failed attempts to initiate a payment that allows the clients to identify fraudulent or malicious use of their accounts.

67. In exchanging client data they shall be protected by encryption techniques. In exchanging client data they may be not encrypted, in case information does not contain data of another client and the client is aware of potential risks.

68. A market participant shall use at least one-element client authentication for:

68.1. a service that allows to view only the client account information that does not contain any third-party data, including account balance, transaction history, account number;

68.2. service related to dealing with financial instruments (sale/purchase).

69. Client log-in access shall be blocked after no more than five failed log-in authentication attempts. Reactivating of client log-in access shall be carried out in a safe manner.

70. Customer's inactive payment session shall be blocked after the time period of no longer than fifteen minutes..

71. As part of client security awareness a market participant shall provide the clients with adequate information about the risks associated with using remote services and information as well as about the secure and efficient use of the IS. Before granting access to remote services to a client and onward, a market participant shall regularly inform a client about the rights and responsibilities of market participant and client, as well as the use of service, security measures required on the side of client (including at the client workstation, mobile device), the secure use of authentication tools and the procedures to follow in case of their loss and to identify possible fraudulent transactions, including money mule risks.

72. Communicating with a client, a market participant shall assess content of information and use a secure communication channel if necessary.

73. Prior to the implementation of remote services and with new threats occurring or making essential changes in the IS, a market participant shall perform security checks and tests and improve security measures without undue delay.

74. A market participant shall store audit trails on the client's successful and refused/denied connections for remote services for at least 18 months (including the source IP address, time) and all information necessary for identifying transactions and other activities performed by the end-user.

XI. IS Development and Change Management

75. A market participant shall be responsible for the IS development and change management processes in order to minimise the IS security risks both for the projected IS and other related IS.

76. A market participant shall set processes of IS development, acquisition, testing, implementation and change management.

77. Inception of IS development

77.1. A market participant shall designate persons responsible for the IS project, as well as designate the resource owners of the developed IS in accordance with the Regulations.

77.2. Responsible persons shall perform risk analysis of the IS project and those IS whose operations may be influenced by the new IS, as well as set the IS security requirements and risk restriction measures.

77.3. In setting IS requirements a method shall be used that is applied in incorporating detective and reactive controls (security by design) in the system's architecture and maintenance processes. Security architecture shall envisage a multi-level security system that would ensure the maintenance of overall IS safeguard also in case any of security levels is compromised.

78. IS development

78.1. IS development environment shall be separated from the user environment.

78.2. Each IS shall be recorded. Documentation shall include the necessary amount of information required to carry out high quality application, maintenance and change management of IS, (for example, the IS description, IS administrator and end-user manuals, etc.).

78.3. A market participant shall store and use documentation in accordance with the classification level of the documentation.

79. IS testing

79.1. Prior to implementing the IS, a market participant shall perform testing of the IS according to a plan. The test plan shall include also the IS security test, including the IS security test, in which testing shall be performed that include potential attack scenarios based on the observed security threats and changes made.

79.2. A market participant shall separate the IS test environment from the user environment.

79.3. Data of user environment shall not be used in testing environment and development environment; however, if for the IS risk minimising purposes, the user environment data is required to use in testing environment or development environment, the same security measures shall be applied and data shall be used in the same manner as for the user environment (including procedures for granting rights, authentication, auditing).

80. IS implementation

80.1. Prior to implementing the IS, permission of IS resource owners shall be received verifying that testing is completed and the IS is prepared for implementation.

80.2. Before putting the IS into operation a market participant shall conduct training of employees.

80.3. A market participant shall ensure the IS versions control.

81. Change management

81.1. Changes in the IS shall be carried out only with the permission of relevant IS resource owners.

81.2. A market participant shall analyse how the changes will affect the existing IS security measures and information available due to granted rights and if the changes will not diminish the level of IS security.

81.3. A market participant shall supplement the IS documentation.

81.4. A market participant shall prepare the rules for activities in the situation of emergency (unplanned) changes and shall assign persons authorised to make a decision on emergency changes. A market participant shall determine the planning of measures to prevent the necessity for emergency changes and shall take the measures to prevent from carrying out unauthorized changes.

82. Terminating the IS use, liquidating or transferring it to another person, including in cases when a market participant terminates any type of business activity, supported by the IS, a market participant shall carry out the necessary security measures, including risk analysis.

XII. Incident management

83. The purpose of incident management shall be to minimise an impact of the IS security incidents on the market participants and operation of market participants as well as to minimise the risk of incident recurrence.

84. A market participant shall determine and implement the IS security incident management process which covers at least:

84.1. identifying the IS security incidents;

84.2. minimising the impact and consequences of incident;

84.3. registering incidents in the incident register;

84.4. analysis of the occurred IS security incident (*inter alia* determining root cause and risk mitigating measures) and reporting to the management;

84.5. saving data for digital forensic process.

85. Payment service providers, which are credit institutions established in Latvia, authorised payment institutions and authorised electronic money institutions, shall report major incidents in accordance with the Financial and Capital Market Commission's Regulations No 157 "Regulations on Major Incidents Reporting related to Payment Services" of 26 September 2018.

86. Recovery of the IS functions

86.1. A market participant shall ensure timely recovery of the IS functions and data in case of IS operational interruptions.

86.2. A market participant shall develop the IS operational recovery plan in accordance with its business continuity plan. A market participant shall take into account potential adverse scenarios it might be exposed to.

86.3. Recoverable IS services shall be included in the IS functions recovery plan in order of priority, as well as available resources, list of planned activities and responsible employees.

86.4. Under the procedure set beforehand, a market participant shall regularly conduct training of persons engaged in the IS function recovery processes and shall document testing under the relevant scenarios and update the plan in case of any changes.

87. In the event of a disruption or emergency and during the implementation of the business continuity plans, a market participant shall have effective crisis communication measures in place so that all relevant internal and external stakeholders, including outsourcing service providers, are informed in a timely and appropriate manner.

XIII. Closing provision

88. Upon these Regulations take effect the Regulations No 112 on Information Systems Security for Participants of the Financial and Capital Market of 7 July 2015 shall become null and void.

Deputy Chairwoman G. Razāne
Financial and Capital Market Commission