Pursuant to Article 158-j, Point 1), of the Law on Insurance Supervision – consolidated text (Official Gazette of the Republic of Macedonia No. 30/2012), Decision of the Constitutional Court No. 202/2011 (Official Gazette of the Republic of Macedonia No. 45/2012), Decision of the Constitutional Court No. 130/2011 (Official Gazette of the Republic of Macedonia No. 60/2012), Decision of the Constitutional Court No. 122/2011 (Official Gazette of the Republic of Macedonia No. 64/2012) and Decision of the Constitutional Court No. 129/2011 (Official Gazette of the Republic of Macedonia No. 23/2013), the Council of Experts of the Insurance Supervision Agency adopted the following

RULEBOOK

ON THE MINIMUM STANDARDS OF THE INFORMATION SYSTEMS OF THE INSURANCE UNDERTAKINGS

I. General Provisions

Article 1

(1) This Rulebook prescribes the minimum standards that are to be met in the operation of the information systems of the insurance undertakings (hereinafter: the Undertakings).

(2) The prescribed minimum standards referred to in Paragraph (1) of this Article shall refer to the management, security and operation of the information systems of the Undertakings, and to the provision of continuity in operation in case of a disastrous event.

II. Information Systems Management

Article 2

The Undertakings shall be required to set up an adequate information system that will meet the following requirements:

1. To have the corresponding functionalities, capacities and performances that will enable the carrying out of the business processes.
2. To provide timely, accurate and complete information that are necessary for everyday operations and for the decision-making in the Undertaking. and
3. To include the necessary controls for data entry, processing and output of the processed data, which will enable the prevention or detection of flaws or inconsistencies in the data or information.

Article 3

The Undertaking shall be required to supervise, revise and continuously to improve the information system, and the process of management thereof, so as to ensure an adequate functionality of the system in compliance with the requirements referred to in Article 2 of this Rulebook.

Article 4

The Undertaking shall be required to define an organisational structure that will define the tasks and responsibilities of all the employees participating in the operation, maintenance and improvement of the information system.

Article 5

The Undertaking shall be required to ensure the enforcement of all the adopted internal acts and procedures relating to the information system, and also to ensure all the information system users to be informed about the contents of these acts and procedures in accordance with their authorisations, responsibilities and needs.

Article 6

(1) The Undertaking shall be required to adopt an information system development strategy as a separate document within the general development strategy, which will be in compliance with the operational needs of the Undertaking.

(2) The Undertaking shall be required to revise this strategy and harmonise it with the changes in the Undertaking's operations.

Article 7

The Undertaking shall be required to prepare and prescribe a methodology that will help define the criteria, methods and procedures for the management of projects related to the information system.

III. Risks Management

Article 8

The Undertaking shall be required to set up a risks management process for the information system risks which shall include risk identification and evaluation, and undertaking of measures for their elimination, mitigation or transfer.

Article 9

The Undertaking shall be required to prepare and prescribe a risk analysis and evaluation methodology for the information system risks. The methodology shall clearly define the system for risk magnitude determination (analysis) and the process of risk comparison according to it probability criteria, so as to determine the significance of the risk (evaluation).

Article 10

The Undertaking shall prepare and prescribe an adequate document "Risk Register" where the information will be stored about the identified risks, and the measures that have been proposed and undertaking for their elimination, mitigation and transfer.

Article 11

(1) The Undertaking shall be required to set up an Information System Risk Committee (hereinafter: the Risks Committee) which will carry out the activities set forth by the information system risks management process i.e. it will identify, analyse and evaluate the risks and will propose measures for their elimination, mitigation and transfer, it will update the "Risk Register" and will verify the implementation of the proposed measures.

(2) The Risk Committee shall comprise at least two members. The Information System Risk Committee shall mandatorily include the person in charge of the information system.

(3) In case the Undertaking has set up a risk committee that covers all the operational risks, this committee can also perform the function of the Information System Risk Committee so long as this committee includes the person in charge of the information system as its member.

Article 12

The Risk Committee shall be required to make a regular analysis and evaluation of the information system risks and to update the "Risk Register", at least twice a year.

Article 13

The Risk Committee shall be required to include in the risk management process all the new projects related to the information system as early as in the stage of their project design.

Article 14

The Risk Committee shall be required to report on its work, after every meeting held, to the Undertaking's managing body. The Report shall also include an updated Risk Register.

Article 15

The risk elimination, mitigation and transfer measures proposed by the Risk Committee shall be implemented only if they are adopted by the Undertaking's managing body.

IV. Security of the Information System

Article 16

(1) The Undertaking, depending on the complexity of the information system, shall be required to prepare and prescribe the information system security policy.

(2) The information system security policy shall define the principles, methods and procedures used for the accomplishment of an adequate level of security as well as the responsibilities and authorisations of all users with regards to the information system security and resources.

(3) The Undertaking shall b required to update its information system security policy in accordance with the changes in the surrounding and the changes in the information system itself.

Article 17

(1) The Undertaking shall be required to establish a continuous process of information system security management. This process shall identify the potential security deficiencies of the information system, register all the security incidents and implement controls which will eliminate these security deficiencies and will ensure an adequate level of information system security.

(2) The security management process shall mandatorily take into consideration also the security risks arising from the very risks management process.

Article 18

(1) The Undertaking shall be required to implement adequate controls of access to the information system resources, and also to implement an adequate management system for the user access rights.

(2) The user rights management system shall implement the processes of identification, authorisation and authentication of the users, record-keeping of the users and their activity in the information system, as well as supervision over the management (allocation and revocation) of the user rights.

(3) The Undertaking shall be required to allocate the user rights based on the principle of allocating the least privilege necessary for the smooth execution of the work assignments.

(4) The Undertaking shall be required to verify the user rights periodically or as required, but at least once a year.

(5) The Undertaking shall be required to ensure a high level of security of users who have an external access to the information system, at least by implementing an encrypted connection and a 2-factor authentication.

Article 19

(1) The Undertaking shall be required to set up and implement a process of creation and storing of a back-up copy of the information system data.

(2) The Undertaking shall be required to prepare and prescribe a procedure for creation and storing of a back-up copy of the information system data, including: Data necessary for the business operation of the Undertaking, the records from the user rights management system, as well as the back-up copy of the application i.e. their installation files which are used as part of the information system.

(3) The procedure for the creation and storing of the back-up copy shall in detail describe the resources for which such a copy is produced, the methods and the frequency of the creation of such copies, as well as the storage location and duration.

(4) The Undertaking shall be required to keep records of the created copies and to carry out periodic testing of the media on which the back-up copies are stored, as well as the process of retrieving the data from the back-up copy at least once a year.

(5) The back-up copies that are stored outside of the Undertaking's facilities shall mandatorily be encrypted.

V. Business Continuity Management

Article 20

The Undertaking shall be required to set up a business continuity management process with the aim to ensure smooth and continuous functioning of all the critical systems and processes, and to restrict the losses in case of emergency operations.

Article 21

(1) The Undertaking shall be required to manage its business continuity based on the developed business impact analysis and risks assessment, which shall include:

1. Definition of th critical business processes necessary for the smooth and continuous functioning of the Undertaking;
2. Definition of the resources and systems necessary for the execution of individual business processes, as well as their interrelations and interdependencies.;
3. The risk assessment for each individual business process as well as the probability of occurrence of the undesired events and their impact on the continuity of the Undertaking's operations, financial losses and reputation;
4. Definition of the level of acceptable risks ad the risk mitigation and identification techniques;
5. Definition of the longest acceptable discontinuation of operations for each process.

(2) Based on the analysis made, the Undertaking shall be required to adopt a business continuity strategy, which shall define the following:

1. Priorities for recovering the business processes back to function, as well as the necessary resources and systems for that purpose;
2. The required capacity levels for the business processes (Service Delivery Objective, SDO);
3. The required time to recover the business processes (Recovery Time Objective, RTO); and
4. Point in time of recovering the business processes (Recovery Point Objective, RPO).

(3) The business continuity strategy shall be adopted by the managing body of the Undertaking.

Article 22

(1) The Undertaking shall be required, based on its adopted business continuity strategy referred to in Article 21, to prepare and adopt a business continuity plan which shall include:

1. Description of the procedures in case of discontinuation of operations, including the manner in which the plan comes into force;
2. A list of identified critical processes according to the business continuity strategy, as well as their SDO, RTO and RPO;
3. Updated list of necessary resources for setting up business continuity;
4. Update contact information about the persons involved in the implementation of the business continuity plan, as well as their tasks and responsibilities.

5. Adequate procedures for restoration of the information systems necessary to support the business processes set forth in the business continuity plan.

(2) The business continuity plan shall be adopted by the managing body of the Undertaking.

Article 23

The Undertaking shall be required to prepare an adequate procedures for restoration of the information systems which are necessary to support the business processes set forth in the business continuity plan. These procedures shall constitute an integral part of the continuity plan, and they should include:

1. List of necessary resources for the restoration of the information system and the corresponding subsystems;
2. List of persons who will be involved in the restoration of the information system or adequate subsystmes, with their tasks and liabilities;
3. A procedure/guidelines for the restoration of the information system or corresponding subsystems with a detailed description of all the steps necessary for the restoration of its operation.

Article 24

The Undertaking shall be required to update and revise the business continuity analysis, strategy and plan periodically or as required, but at least once in two years.

Article 25

(1) The Undertaking shall be required to test the continuity plan periodically or as required, but at least once in two years. The testing shall be carried in such a way that the functionality of the plan under real circumstances can be verified.

(2) The Undertaking shall be required to prepare minutes from the testing of the continuity plan and make the necessary corrections to the plan according to the identified deficiencies.

(3) The minutes from the testing of the business continuity plan shall be adopted by the managing body of the Undertaking.

Article 26

The Undertaking shall be required to inform regularly all the persons involved in the business continuity plan about its contents and amendments, in compliance with their tasks and responsibilities in the implementation thereof.

VI. External Information Technologies Service Providers Management

Article 27

(1) The Undertaking shall be required to set up a management process for services delivered by external service providers of information technologies (hereinafter: IT services). The aim

of this process shall be to set up adequate decision-making procedures when selecting the supplier, managing the service level, and fulfilment of the service level agreement by the supplier.

(2) Such services as the procurement and maintenance of IT equipment, telecommunication services and ready-made software commercially available on the market (off-the-shelf) shall not be subject to this process.

Article 28

The Undertaking shall be required to prepare and adopt decision-making procedures for the selection of IT services supplier, which will mandatorily include:

1. Analysis of the potential IT services suppliers with regards to their technical capacities to provide the required service, financial position of the supplier and its business reputation;
2. In case the supplier is from another country or countries, verification as to whether the regulations of those countries ensure adequate control of the supplier's operations by the Insurance Supervision Agency for the IT services to be delivered to the Undertaking; and
3. Analysis of challenges and the time required for selection of another supplier, or possibilities for delivery of the same services by the undertaking itself, in case of discontinuation of the service provision by the supplier.

Article 29

The Undertaking shall be required to prepare and adopt a management procedure for the service level of the IT services supplier, which will mandatorily include:

1. Regulation of the licencing rights, source code ownership, as well as the rights to intellectual property;
2. Regulation of the rights to overtaking the source code rights in cases where the supplier is not in the position ot deliver the service (escrow arrangement);
3. Regulation of the rights to inspection and control of the operation of the IT services supplier for specific service subject to a contract with the Undertaking;
4. Regulation of service level parameters;
5. Regulation of the reporting method about the accomplished service level; and
6. Regulation of the verification and monitoring of the compliance of the IT services supplier with the legal provisions.

Article 30

Contracts that the Undertaking concludes with the IT services supplier, which, inter alia, include processing, storing and access to the Undertaking's data, shall mandatorily contain the following elements:

1. Provisions about the clear distinction of the rights and responsibilities between the Undertaking and the IT services supplier;
2. Provisions for the definition of the possibilities for early termination of the contractual

obligations;

3. Provisions for the compliance of the supplier with the corresponding legal regulations;
4. Provisions for the confidentiality of information;
5. Provisions that enable the Undertaking to have smooth access to and control options over the supplier's premises and data, with regards to the services delivered on the behalf of the institution.

With the contract the Undertaking shall ensure a smooth access to and control options over the premises and data of external persons and ISA, as well as for the Audit Company that will make the audit of the annual financial statements of the institution.

Thereby, access shall only refer to the data relating to services provided by an external person for the Undertaking.

VII. Transitional and Final Provisions

This Rulebook shall enter into force on the day of its promulgation in the "Official Gazette of the Republic of Macedonia" and shall become effective as of 1 January 2015.

No. 0201-1258/9

19.12.2013

Skopje

President of the Council of Experts,

Dr. Klime Poposki