Pursuant to Article 158-b paragraph (1) point 4 and Article 158-j point (1) and in connection with Article 32 paragraph (1) point 13), Article 134-f paragraph (2) point 9) and Article 146 paragraph (2) point 9) of the Law on Insurance Supervision ("Official Gazette of the Republic of Macedonia" no. 27/02, 84/02, 98/02, 33/04, 88/05, 79/07, 08/08, 88/08, 56/09, 67/10, 44/11, 88/13, 43/14, 12/14, 153/15, 192/15, 23/16, 83/2018 198/18 and "Official Gazette of the Republic of North Macedonia" no. 101/19 and 31/20), the Council of Experts of the Insurance Supervision Agency at the meeting held on 22.10.2020 adopted the following:

RULEBOOK ON
the minimum test standards for the information systems of insurance companies, insurance brokerage companies and insurance representation companies

I. General provisions
Article 1

This rulebook prescribes the minimum standards of the information systems of insurance companies, insurance brokerage companies and insurance representation companies.

Article 2

The minimum standards of information systems of insurance companies, insurance brokerage companies and insurance representation companies refer to the organizational set-up of the Information System Service, the management of the information system, the infrastructure of the information system, the main business system, the security of the information system, the management and business continuity of the information system, management of services in the field of information technologies, procurement of services in the field of information technologies and training for employees in the information system service.

II. Information system of insurance companies
Article 3

(1) The insurance company is obliged to establish an information system as a basic tool for the performance of its daily operations.

(2) The insurance company must have adopted internal procedures/rules and establish a system of internal controls to monitor the compliance of the company's operations with the provisions of these rules and legal regulations.

(3) The internal control system in accordance with paragraph (2) of this article should function throughout the company's operations in continuity, and the management and supervision bodies of the insurance company must establish instruments for measuring the efficiency and effectiveness of the functioning of the internal control system in order to improve it.

(4) The insurance company should perform documented internal evaluations of the functioning of the system of internal controls at least once a year.

(5) The absence i.e. the serious deficiencies in the functioning of the system of internal controls intended by the provisions of this regulation is considered to be a deterioration in the risk management of the insurance company intended to comply with the provisions of the Law on Insurance Supervision, which relate to risk management.

Organizational set-up of the functions for development and support of the information system
Article 4

(1) The insurance company is obliged in the external organization act to establish an organizational form responsible for the development and support of the information system, and in the act for the systematization of workplaces, it defines at least an adequate description and list of work tasks for each foreseen workplace in that organizational form.

(2) The insurance company is obliged to continuously have a manager of the organization form in charge of the development and support of the information system, a full-time employee.

(3) In case of termination of the employment relationship of the manager, for any reason, the company is obliged immediately, and no later than within three months from the termination of the employment relationship, to appoint a new manager in charge of development and support of the information system.

Managing the information system
Article 5

(1) The insurance company is obliged to continuously adopt a strategic plan for the development and support of the information system.

(2) The strategic plan from paragraph (1) of this article should cover a period of at least 3 and at most 4 years and contain at least:
- Review of the state of the information system at the beginning of the period;
- clearly defined and measurable strategic priorities and goals that will be achieved at the end of the period;
- an action plan for achieving the goals and priorities in which at least the activities, the holders of the activity, the participants in the activity, the start of the execution of the activity, the deadline for completing the activity and the budget for each activity will be clearly and precisely defined.

(3) The strategic plan from paragraph (1) of this article shall be adopted no later than the end of the first quarter of the initial year of its validity.

(4) The strategic plan from paragraph (1) of this article can be changed and supplemented during the validity period, if the need arises.

Project management methodology
Article 6

(1) The insurance company is obliged to adopt a project management methodology related to the development and support of the information system.

(2) The project management methodology from paragraph (1) of this article should describe in detail the project management phases of the company: initiation, planning, execution and closure and be in line with some of the world's most applied methodologies in the field (PMI, Prince 2, Agile, Scrum).

Information and communication infrastructure
Article 7

(1) The insurance company is obliged to provide adequate conditions for accommodation and storage of critical components of the information infrastructure such as servers, storage devices, security devices, network equipment etc.

(2) The critical components of the information infrastructure should be located in a separate room/s with controlled access, which will provide protection against physical threats such as: theft, fire, explosions, smoke, flood, dust, vibrations, chemicals, obstacles in the supply of electricity, communication obstacles, basic electromagnetic influences and vandalism. The right of access to the room/s should be limited only to the employees who have competence in the area, and for the access, electronic records should be kept at each entrance to the room.

(3) The room where the critical components are located should constantly have a controlled operating temperature and humidity.

Location of critical components
Article 8

At least one location (production or reserve) of the critical components of the infrastructure should be located on the territory of the Republic of North Macedonia or a member state of the European Union.

Main business system
Article 9

(1) The insurance company is obliged to implement the main business system as a basic part of the information system.

(2) The main business system from paragraph (1) of this Article should be an integrated system, which will ensure fully digitized execution of work processes; timely, accurate and complete information, for the operations and decision-making of the insurance company, with implemented and appropriate controls in data entry and processing; and which contain the following functional modules:

- Human resources management – organizational chart, jobs, personnel records, job allocation, employment contracts, disciplinary measures, evaluation;
- Financial operations;
- Financial accounting – general ledger with automatic postings based on pre-defined posting patterns, generating accounting balances at any time;
- Salaries and personal income tax;
- Material operations;
- Fixed assets;
- Travel orders;
- Treasury;

- Financial operations;
- Penalty interests and warnings;
- Standard purchases;
- Budgeting and cost management - Formation of the budget, monitoring of the execution of the budget, possibilities of reassignment and rebalancing;
- Lawsuits – registration of lawsuits, generator of lawsuits, follow-up of lawsuits;
- Admission to insurance;
- Management of the sale of policies - creation, generation, printing of insurance policies and automatic invoicing of policies;
- Approval of policies;
- Sales through other companies;
- Customer relations - management of detailed customer files of all active and passive customers;
- Damages;
- Recourse claims - recourse referencing one or more paid damages
- Book of damages – records of damages;
- Damages management - Registering the damages through the formation of cases and recording all related events and procedures by attaching the appropriate, previously digitized documentation (from application to payment);
- Reinsurance – Registering, documenting, executing and monitoring reinsurance operations (portfolio or individually);
- Investment portfolio – registering, recording and monitoring the investment
- Reports: a wide range of pre-defined quality reports and the possibility of creating add-on reports (one or more dimensional), combining reports with the regulator according to the requirements.

(3) The main business system from paragraph (1) of this Article should enable automatic booking on a predefined basis everywhere and from each module, whereever possible; Management of work processes (Workflow) within the framework of the entire system, with implemented digital work with documents, i.e. scanning of all documents and appropriate attachment for work process (Single Document Entry principle), as well as automatic generation of cases wherever possible and necessary; Generators of documentation based on predefined patterns wherever possible. The system should include a user activity log at the application level, which will record all the activities performed in the system by each of its users and the time when they were performed.

(4) The main business system in paragraph (1) of this Article must be in accordance with the legal regulations in the Republic of North Macedonia of the respective areas that it covers.

System integration
Article 10

(1) The insurance company can integrate its Main Business System with other external information systems in the field of insurance in order to improve its operations.

(2) The integration of the systems should be achieved synchronously, that is, online, using the appropriate API (Application Programming Interface) or other technologies that will enable equivalent functionality and compliance with security standards.

(3) The insurance company is obliged to prepare the appropriate documentation for the method of integration and deliver it to the interested parties, if an agreement on business cooperation is reached.

Official website
Article 11

The insurance company is obliged to establish an official website for the performance of its functions.

Security of the information system
Article 12

The insurance company is obliged to establish a continuous process for managing the security of the information system, which will enable the highest required level of security of the system.

Procedure for users
Article 13

(1) The insurance company is obliged to prescribe a procedure for user names, passwords and user rights; which will contain at least the following: form of the user name, form of the password, period of change, unrepeatability of the password, resetting of the password, suspension of the user, and a description of user rights that should correspond to the work tasks of the user.

(2) The insurance company is obliged to ensure an encrypted connection with modern encryption and multi-factor authentication for users who access the system via the Internet.

(3) The insurance company is obliged to continuously maintain an up-to-date list of users and user rights.

(4) The insurance company is obliged to check user rights at least once every six months of the year and to prepare a report.

Information system risk management
Article 14

(1) The insurance company is obliged to establish an efficient process for managing the risks of the information system, which will include the identification and evaluation of the risks as well as taking measures for their removal, mitigation or transfer.

(2) The insurance company is obliged to prescribe a methodology for managing the risks of the information system.

(3) The insurance company is obliged to establish a "Register of Risks" which should be continuously updated and contain a list of risks from at least the following areas: infrastructure, external and internal threats (malicious code, unauthorized intrusions from the inside and outside, etc.), human factor, natural disasters. For each risk, it is necessary to determine at least an assessment of the probability of occurrence, an assessment of the possible harmful impact, a way of dealing with it and the resources needed to deal with it.

(4) The insurance company is obliged to form a Risk Committee of the information system, which is managed by the head of the organizational form for the development and support of the information system, and in which there are at least two members from among the employees of the company or from the group to which the company belongs. The insurance company can also hire external experts as members of the Board, who should have competencies for risk management of information systems proven by a CRISC (Certified in Risk and Information Systems Control) certificate or equivalent. With the members of the board for risks that are not employees of the insurance company, an agreement must be signed, in which the obligations and rights of both parties will be defined. The board performs all the necessary tasks for the management of the risks of the information system.

(5) The risk committee from paragraph (4) of this Article is obliged to hold at least one quarterly meeting. At each meeting, a Proposal - Register of risks must be established. According to the proposal, the management body of the company is obliged to adopt a decision at its next meeting.

Back-up
Article 15

(1) The insurance company is obliged to establish and implement a process of creating and keeping a back-up copy of the information system data.

(2) The insurance company is obliged to adopt a procedure for creating and keeping a back-up copy of the information system data, which will contain at least: data necessary for the company's business operations, records from the user rights management system, a back-up copy of the applications themselves, i.e. their installation files used as part of the information system, as well as data recovery from the back-up.

(3) In addition to the provisions of paragraph (2) of this Article, the procedure for creating and keeping a back-up copy should describe in detail the resources for which such a copy is made, the ways in which it is done, the frequency of making these copies, as well as the duration and place where they are stored.

(4) The insurance company is obliged to keep a back-up copy of the data in a safe location outside the company's premises where the information infrastructure is located.

(5) Back-up copies that are kept outside the premises of the company must be encrypted.

(6) The insurance company is obliged to continuously keep records of the created copies and at least once in each half of the year, to periodically test the media on which the back-up copies are kept.

(7) The insurance company is obliged to test the data recovery process from the back-up copy at least once a year, for which a report is drawn up.

Information system protection
Article 16

(1) The insurance company is obliged to provide quality protection of the information system against external and internal threats (eg malicious codes, SQL injection, intrusion, phishing, DoS, etc.)

(2) The insurance company is obliged to establish a process of continuous collection and analysis of information related to new weaknesses in its infrastructure. It should compare these weaknesses with current threats to the security of the information system and take actions to overcome them as soon as possible according to the weakness and the threat.

(3) The insurance company is obliged to define the way of managing security upgrades, upgrades to new versions, changes to the parameters and code of the components of the information system, as well as the preparation and putting it into use. For all these changes, as well as for incidents and problems, it is necessary for the company to have records of the entire process from registration, change request, approval, testing and resolution.

(4) The insurance company is obliged to prescribe a protection procedure that will describe at least what solutions are used; as well as how often solutions are updated on the server and client side; as well as how often the server and client computers are checked and how the users of the system should act in case of possible suspicious situations.

(5) The insurance company is obliged to control the implementation of the procedure at least once every six months of the year and to prepare a report for the same, which should include a record of all possible incidents or attempts related to the above-described protection of the system.

(6) The insurance company is obliged at least once every two years to hire external experts or a legal entity that will conduct a penetration test procedure on the information system. The scope of this testing should include at least all public IP addresses and applications accessible from public URLs even in cases where they are used through encrypted or authenticated channels, the main business system (including databases and operating systems), critical network components and wireless networks.

(7) The persons or legal entity performing a penetration test should have competencies that are proven by holding certificates and have professionals in the team who hold one of the following certificates: CEH, CEH Master, Lead Pentest Professional, OSWP according to the type and complexity of the infrastructure to be tested.

(8) Individuals or legal entities should submit to the insurance company a report from the test, with recommendations for overcoming any identified vulnerabilities of the system.

(9) In the event that the insurance company uses applications, i.e. systems, which are implemented and hosted in the corporate infrastructure, the penetration test should be conducted by the corporation. The insurance company is required to provide a test report.

Employee trainings
Article 17

(1) The insurance company is obliged to adopt an Annual training plan for the protection of the information system for all employees who use the system. The purpose of the trainings is to increase the level of awareness among employees about the security of the information system and to give them basic knowledge for dealing with potential threats.

(2) The insurance company is obliged to control the implementation of the annual training plan for the year, for which it prepares a report no later than the end of the first quarter of the business year for the previous business year.

Business Continuity Management
Article 18

(1) The insurance company is obliged to establish a business continuity management process in order to ensure smooth and continuous functioning of all critical systems and processes, as well as to limit losses in conditions of extraordinary operation.

(2) The insurance company is obliged to manage the business continuity based on an analysis of the impacts of the operation and an assessment of the risks, which should include at least: Defining the critical business processes necessary for the smooth and continuous functioning of the company; Defining the resources and the systems needed to perform the individual business processes, as well as their interdependencies and connections; Risk assessment for each of the individual business processes, as well as the probability of the occurrence of unwanted events and their impact on the continuity of operations, financial losses and the reputation of the company; Defining the level of acceptable risks and the techniques to mitigate the identified risks; Defining the longest acceptable interruption of operation for each of the processes.

(3) Based on the analysis, the insurance company is obliged to adopt a business continuity strategy, which will define at least the following:

- The priorities of returning to function of business processes, as well as the necessary resources and systems for that purpose;
- Levels of required capacity of business processes (RCBP);
- Necessary turnaround time for business processes (NTT) and
- Defining a necessary point of return of business processes (NPR).

Business continuity strategy is adopted by the management body of the insurance company.
Article 19

(1) The insurance company is obliged, based on the adopted business continuity strategy from Article 18 of this regulation, to prepare and adopt a business continuity plan that will contain at least:

- Description of the procedures in case of cessation of operations, including the method of entry into force of the plan;
- List of identified critical processes according to the business continuity strategy, as well as their RCBP, NTT and NPR;
- Updated list of resources needed to establish business continuity;
- Updated contact information for the persons participating in the implementation of the continuity plan, as well as their tasks and responsibilities.

- Adequate procedures for rebuilding the information systems that are necessary to support the business processes foreseen by the business continuity plan.

(2) The business continuity plan from paragraph (1) of this Article is adopted by the management body of the insurance company.

Procedures for restoration of information systems
Article 20

(1) The insurance company is obliged to prepare appropriate procedures for the reconstruction of the information systems that are necessary to support the business processes foreseen by the business continuity plan of the company.

(2) The procedures from paragraph (1) of this Article are part of the Continuity Plan and they should contain at least the following:
- List of necessary resources needed for the reconstruction of the information system or the corresponding subsystem;
- List of persons who will participate in the reconstruction of the information system or the corresponding subsystem, with their tasks and obligations;
- Procedure/guideline for rebuilding the information system or the corresponding subsystem with a detailed description of all the steps needed to restore its operation.

Revising the analysis, strategy and business continuity plan
Article 21

The insurance company is obliged to update and revise the analysis, strategy and business continuity plan at least once, every two years.

Continuity plan testing
Article 22

(1) The insurance company is obliged to fully test the continuity plan at least once every two years. The scenarios that will be tested should cover different threats that will not be repeated in order for the testing to be productive in terms of improving the business continuity plan.

(2) The insurance company is obliged to prepare minutes from the testing of the continuity plan, and to make appropriate corrections to the plan according to the observed deficiencies.

(3) The minutes from the testing of the business continuity plan are adopted by the management body of the insurance company.

Article 23

The company is obliged to regularly inform all persons participating in the business continuity plan about its content and changes, according to their tasks and responsibilities in the implementation of the plan.

Management of information technology services from external suppliers
Article 24

The insurance company is obliged to establish a service management process from external providers of information technology services (hereinafter referred to as IT services). The purpose of this process

is to establish appropriate decision-making procedures during the selection of the supplier, management of the service level, as well as the fulfillment of the agreed level by the supplier. Services such as: procurement and maintenance of IT equipment, telephony services and procurement of ready-made software that is commercially available on the market (off-the-shelf) are not subject to this process.

Procedure for managing the level of service of an IT service provider
Article 25

(1) The insurance company is obliged to prepare and adopt a procedure for managing the level of service of an IT service provider, whereby, using the best global practices in the field, it will obligatorily overlook at least the following:

- Arrangement of licensing rights, ownership of source code, such as intellectual property rights;
- Arranging the rights to take over the rights to the source code in cases where the supplier is unable to deliver the service (escrow arrangement);
- Arranging the rights to inspect and control the operation of the supplier of IT services for the specific service that is the subject of the contract with the company; Defining the parameters for the level of service;
- Defining the method of reporting the achieved level of service;
- Defining steps and measures in case of deviation from the agreed service level by the service provider;

Ensuring full access to the resources, information and documentation of the company at the external supplier of the external auditor as well as the Insurance Supervision Agency.

(2) An integral part of the procedure can be a model contract for managing the level of service.

Implementation of procurement of information technologies
Article 26

The insurance company is obliged to prescribe a procedure for the procurement of IT equipment, licenses, application software and IT services, which describes in detail at least the following: the process of internal approval of the procurement, the preparation of the necessary technical and functional specifications for the subject of procurement, the method and deadline for collecting bids, the method of evaluating the bids and notifying the selected bidder.

Employees training in the organizational form for development and support of the information system
Article 27

(1) The insurance company is obliged to continuously provide training to employees in the organizational form for the development and support of the information system.

(2) In function of conducting the trainings, the insurance company is obliged to adopt an annual training plan, based on a previous analysis of training needs, no later than the end of the first quarter of the business year.

(3) Managerial skills training (human resource management, management of daily activities, project management, strategic planning, risk management, etc.) must be provided for the head of the organizational form, and for all employees in the organizational form at least training on the technologies used in the work.

(4) The insurance company is obliged to prepare a report of conducted trainings, no later than the end of the first quarter of the current business year for the previous business year.

Submission of documentation to the Agency
Article 28

The insurance company is obliged to submit the documentation from Articles 3, 5, 13, 14, 15, 16, 17, 21, 22 and 27 to the Insurance Supervision Agency no later than within five working days of the appropriate term prescribed for its adoption.

II. Information system in insurance representation companies and insurance brokerage companies

Information system
Article 29

Insurance representation companies and insurance brokerage companies, except for banks that perform representation operations (hereinafter: companies), are obliged to establish an information system, as a basic tool for performing functions in daily operations.

Main business system
Article 30

(1) The companies are obliged to implement the main business system as a basic part of the information system. The main business system should be an integrated system, which will ensure timely, accurate and complete information about the earnings and decision-making of the company, implemented with appropriate controls and data processing; and will provide predefined reports to the regulator according to the requirements.

(2) The main business system from paragraph (1) of this Article should be in compliance with the legal regulations in the Republic of North Macedonia of the respective areas and areas it covers.

Article 31

The company can also implement other external information systems in the field of insurance in order to improve its operations. These systems should be integrated with the systems of insurance companies, i.e. other entities related to the area. The integration of the systems should be done synchronously, i.e. online, using an appropriate API (Application Programming Interface) or another way of integration that will provide adequate functionality and security protection. The company is obliged to prepare appropriate documentation for the method of integration and provide the same to the parties interested in integration, together with the documentation prepared by the insurance companies and other entities.

Official website
Article 32

The company is obliged to establish an official website for the performance of its functions.

Security of the information system
Article 33

The company is obliged to establish a continuous process for managing the security of the information system, which will enable the highest required level of security of the system.

Back-up
Article 34

(1) The company is obliged to establish and implement a process of creating and keeping a back-up copy of the information system data.

(2) The company is obliged to adopt a procedure for creating and keeping a back-up copy of the data on the information system, of at least the following: the data necessary for the company's business operations, the records from the user rights management system, a back-up copy of the applications themselves, i.e. their installation files used as part of the information system, as well as data recovery from back-up.

(3) The procedure for creating and keeping a back-up copy should describe in detail the resources for which such a copy is prepared, the ways in which it is done, the frequency of making these copies, as well as the duration and place where they are kept.

(4) The company is obliged to keep a back-up copy of the data outside the company's premises where the information infrastructure is located.

(5) Back-up copies that are kept outside the premises of the company must be encrypted.

(6) The company is obliged to continuously keep records of the created copies and at least once a year, to periodically test the media on which the back-up copies are kept.

(7) The company is obliged to test the data recovery process from the back-up copy at least once every two years, for which a report is drawn up.

(8) If the company uses services for outsourcing the information system or parts of it, the obligations of this Article should be fulfilled by the service provider, for which appropriate provisions should be provided in the mutual agreement.

Employee trainings
Article 35

(1) The company is obliged to adopt an Annual Training Plan for the protection of the information system for all employees who use the system. The purpose of the trainings is to increase the level of awareness among employees about the security of the information system and to give them basic knowledge for dealing with potential threats.

(2) The company is obliged to control the implementation of the annual training plan for the year, for which it prepares a report no later than the end of the first quarter of the business year for the previous business year.

Submission of documentation to the Agency
Article 36

The company is obliged to submit the documentation from Articles 34 and 35 of this regulation to the Insurance Supervision Agency at the latest within five working days from the date prescribed for its adoption.

Network of managers of organizational forms in charge of the development and support of the information system
Article 37

(1) In order to improve the conditions in the field of digitization of the insurance industry, a network of managers of organizational forms in charge of the development and support of the information system is established.

(2) The basic goals of the network are: exchange of experiences and information from the field of information technologies and InsurTech; discussion of the conditions of applied information technologies in society; discussion regarding the regulation; proposals and suggestions for improvement; organization of trainings and events; guidelines and indications by the Insurance Supervision Agency to the heads of the organizational forms for development and support of the information system.

(3) The coordination of the work of the network is carried out by the competent service for information technology in the Insurance Supervision Agency. The network should hold regular meetings at least once every quarter of the year, and extraordinary meetings may be convened if necessary.

Transitional and final provisions
Article 38

(1) This Rulebook enters into force the day after its publication in the "Official Gazette of the Republic of North Macedonia", and will be applied from January 1, 2021, except for the provisions of Article 16 paragraphs (6), (7) and (8) which will be applied from January 1, 2022 and the provisions of Articles 9, 10, 30 and 31 which will be applied from January 1, 2023.

(2) With the start of applying this Rulebook, the "Rulebook on the minimum standards of information systems of insurance companies" no. 0201-1258/9 dated 19.12.2013 ("Official Gazette of the Republic of Macedonia" No. 187/2013) ceases to be valid.

No. 01-653/1
22.10.2020 Skopje

President of the Council of Experts
Krste Shajnoski