Pursuant to Article 44 paragraph 2 item 3 of the Central Bank of Montenegro Law (OGM 40/10, 46/10, 06/13, 70/17) and Article 56a paragraph 3 of the Payment System Law (OGM 62/13, 111/22), the Central Bank of Montenegro Council, at its meeting held on 28 April 2023, passed the following

DECISION
ON SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS RELATED TO PAYMENT SERVICES

I. BASIC PROVISIONS

Subject matter

Article 1

(1) This Decision shall specify the security measures for operational and security risks related to payment services, as well as the establishment, implementation and monitoring of security measures.

(2) Within the meaning of this Decision, information system risks (hereinafter: the IS risks) shall be considered operational and security risks.

Proportionality

Article 2

A payment service provider shall comply with the provisions set out in this Decision taking account of, the size, internal organisation, nature, scope, complexity and riskiness of the services and products that it provides or intends to provide.

Application to credit institutions

Article 3

The provisions of this Decision shall apply to credit institutions in the part not governed by the Central Bank of Montenegro's (hereinafter: the Central Bank) decision on minimum standards for managing risks to which a credit institution is or might be exposed to in its operations.

Definitions

Article 4

Terms used in this Decision shall have the following meaning:

1) **information system** (IS) means a comprehensive set of technological infrastructure (software and hardware assets), organisation, people, and procedures for generating, collection, processing, storage, transmission, presentation, use, modification and other procedures for data processing;

2) **IS risk** means the possibility of negative effects on the financial result and capital of a payment service provider, achievement of its business objectives, and operation in accordance with regulations, due to inadequate information system management or other system weaknesses which negatively affect the system functionality or security;
3) **information security** means a state where only authorised users (confidentiality) have access to accurate and complete information (integrity) when they need it (availability);
4) **operational or security incident** means a singular event or a series of linked unplanned events that have or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment services;
5) **confidentiality of information** means that the information is not disclosed or available to unauthorised persons;
6) **integrity of information** means that information i.e. data has not been subject to unauthorised or unforeseen alterations;
7) **availability of information** means that an authorised person may access the information and use it in a timely manner;
8) **information system resources** mean software, hardware and information assets, people and processes;
9) **software assets** (IS software components) mean all types of application and system software, databases, software development tools, utility programmes and other software;
10) **hardware assets** (IS hardware components) mean computers and computer equipment, communication equipment, data storage media and other technical equipment supporting the information system operations;
11) **information assets** means data in databases, data files, program code, configuration of hardware assets, technical and user documentation, reports, strategies, policies, procedures, other internal acts and the like;
12) **information technology (IT)** means a combination of hardware and software assets that enables automated generation, collection, processing, storage, transmission, presentation and/or use of information;
13) **IT system** means information technology governed as a part of the mechanisms or interconnected network that provides support to the payment service provider's operations;
14) **IT service** means any service the IT system provides to internal or external users;
15) **IT project** means any project, or part thereof, where IT systems and services are changed, replaced, dismissed or implemented, and it may be part of wider IT or business transformation programmes;
16) **risk appetite** means the level and types of risk that the payment service provider is willing to assume within its risk capacity to achieve its strategic objectives.

II. MEASURES FOR INFORMATION SYSTEM RISKS RELATED TO PAYMENT SERVICES

Governance system

Article 5

(1) A payment service provider shall make sure that the governance system it shall establish in accordance with the law, which shall include governance structure with clearly defined, evident and consistent lines of powers and responsibilities, provides clearly defined powers and responsibilities for efficient and secure management of the information system (IT operations, IT development, information security, etc.), IS risks and business continuity, and which shall avoid conflict of interest, ensure efficient communication and cooperation regarding the performance of these activities, and establish a clear and documented decision-making process.

(2) A payment service provider shall ensure that an adequate number of persons with necessary professional qualifications and competencies for the performance of activities referred to in paragraph (1) of this Article and for the implementation of the information system development strategy referred to in Article 7 of this Decision is hired on an ongoing basis.

(3) A payment service provider shall prescribe in its internal acts the content, periodicity, and the manner of reporting to its competent bodies on the significant facts regarding the performance of activities referred to in paragraph (1) of this Article.

(4) A payment service provider's organisational parts performing operational activities that incur the IS risks, and in particular the organisational part or parts in charge of IT operations, shall be responsible for establishing adequate processes and controls that, in line with the IS risk appetite, reduce these risks to an acceptable level, as well as for ensuring the compliance of services and systems they provide and the activities they perform with internal and external requirements.

(5) A payment service provider shall designate an organisational part and/or persons directly accountable for coordinating, monitoring and overseeing the application of the IS risk management rules, i.e. ensuring that these risks are identified, measured, assessed, controlled, monitored, and reported.

(6) A payment service provider shall ensure independence and objectivity of the organisational part and/or persons referred to in paragraph (5) of this Article, by ensuring that that organisational part and/or persons do not perform operational activities and tasks that incur risk (that they monitor and oversee), and in particular tasks and activities performed by the payment service provider's organisational part responsible for IT operations.

(7) Organisational part and/or persons referred to in paragraph (5) of this Article shall report to the payment service provider's competent bodies on regular and extraordinary activities related to IS risk management in a timely manner.

Use of third party services

Article 6

(1) A payment service provider shall adequately manage IS risks that arise or that may arise from the business relationship with a third party providing a service or a product in relation to the information system, regardless of whether that business relationship represents outsourcing or not, which shall also include the implementation of risk mitigation measures specified in this Decision.

(2) Payment service provider shall, prior to entering into a business relation referred to in paragraph (1) of this Article, conclude an agreement with the third party regarding such business relation, thereby taking care that the content and scope of contractual provisions are defined in accordance with the complexity and size of activities being entrusted to the third party, and with the IS risk appetite of the payment service provider.

(3) The contract referred to in paragraph (2) of this Article shall contain the provisions regarding, in particular, the following:

1) information security measures including requirements such as minimum cybersecurity requirements, payment service provider's data encryption and life cycle, network security, location of data, requirements regarding the continuity of service provision, system security monitoring, and the like;
2) the manner and dynamic of handling operational and security incidents, including escalation and reporting procedures.

(4) A payment service provider shall monitor the quality and security of the performance of activities that are the subject of the contract referred to in paragraph (2) of this Article and the fulfilment of the agreed service level.

Information system development strategy

Article 7

(1) A payment service provider shall have in place the information system development strategy, for a period of at least three years, which is aligned with the general business strategy and which, at least, should:

1) describe, through a representation of the existing and the desired situation, how the information system should evolve, including the IT system changes, the IT architecture, organisational and operational structure, and the use third party services;
2) define clear information security objectives, focusing on IT systems and IT services, employees and processes;
3) describe the manner in which the payment service provider will commit to information system management with a view to maintaining business continuity.

(2) A payment service provider shall further detail the strategy referred to in paragraph (1) of this Article by adopting annual operational action plans that contain measures to be taken to achieve the objectives defined in the information system development strategy.

(3) The annual operational action plan referred to in paragraph (2) of this Article should, at least, contain the description of activities and projects, contractors, responsible persons, budget and time limits for the execution of planned activities.

(4) A payment service provider shall provide financial resources sufficient for implementing the strategy referred to in paragraph (1) of this Article.

(5) A payment service provider shall establish a processes of continuous measuring and monitoring of the effectiveness of the implementation of the strategy referred to in paragraph (1) of this Article.

Internal acts for IS risk management

Article 8

A payment service provider shall define in its internal acts the rules for IS risk management that shall define at least the following:

1) the IS risk appetite, in accordance with the risk appetite of that payment service provider;
2) the methods and parameters (threat, vulnerability, probability, impact, etc.) for identifying and measuring, i.e. assessing the IS risks to which the payment service provider is exposed;
3) the procedures for defining the risk control measures, including the introduction of new and/or modification of existing controls with a view to mitigating risks;
4) the procedures for monitoring the implementation of measures referred to in item 3) of this Article and their efficiency, as well as the number of identified operational and security incidents, including the incidents reported to the Central Bank in accordance with the law, and taking actions to correct the measures where necessary;
5) the obligation to identify and measure, i.e. assess the risks of a relevant part of the information system resulting from any major change in the information system, services, and/or processes of information system management, before taking a decision on the implementation of such changes;
6) the obligation to identify and measure, i.e. assess the risks of a relevant part of the information system after any significant operational or security incident;
7) the timeframe for conducting regular, comprehensive identification and assessment of IS risks, at least once a year;
8) the manner and periodicity of drawing up and delivering to the competent bodies of the payment service provider the reports on significant facts regarding the IS risk management activities and the exposure of the payment service provider to these risks;
9) the powers and responsibilities for managing IS risks on all work process and decision-making levels, in a way that avoids the conflict of interest.

Mapping of business functions, processes, IT systems, and IT services

Article 9

(1) Payment service provider shall identify and regularly update mapping of its business functions and processes performed within those functions, which shall:

1) describe the interdependences of different functions and processes;

2) contain an overview of information assets used or created by a specific function and/or process;
3) describe outgoing and incoming flow of information between different functions and processes.

(2) A payment service provider shall also identify and regularly update mapping of interdependencies between the business functions and processes referred to in paragraph (1) of this Article and the IT system, IT services, employees and other persons hired by the payment service provider that support and/or enable the functioning of those functions and processes.

Identifying the importance of information system resources

Article 10

(1) A payment service provider shall classify and document business functions, processes and information assets, IT systems, IT services, employees and external service providers referred to in Article 9 of this Decision in terms of their importance, i.e. criticality.

(2) When identifying importance, i.e. criticality of resources referred to in paragraph (1) of this Article, the payment service provider shall, at a minimum, consider the availability, confidentiality, and integrity requirements.

(3) A payment service provider shall clearly define assignments and responsibilities for the resources referred to in paragraph (1) of this Article and their classification.

(4) The importance of resources referred to in paragraph (1) of this Article shall be taken into account when performing the IS risk assessment.

Defining corrective measures

Article 11

(1) Based on the risk assessments results, a payment service provider shall, in accordance with the IS risk appetite, determine which measures are required to mitigate the IS risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, IT systems, and/or IT services.

(2) A payment service provider shall assess the time required to implement the changes referred to in paragraph (1) of this Article and in accordance with IS risk appetite, where appropriate, define interim risk mitigation measures that will apply until the planned changes are carried out.

Audit

Article 12

(1) A payment service provider shall provide the information system audit, and the audit of the information system management and the IS risk management by an independent auditor with sufficient knowledge and experience in the areas of IS risks and payment system.

(2) The frequency and the scope of the audit referred to in paragraph (1) of this Article should be proportionate to the IS risks to which the payment service provider is exposed.

(3) A payment service provider shall adopt and regularly update the audit plan referred to in paragraph (1) of this Article.

(4) A payment service provider shall establish a process in accordance with which the measures for removing the irregularities and deficiencies identified by the audit referred to in paragraph (1) of this Article are implemented, as well as a follow-up of that implementation process.

Information security policy

Article 13

(1) A payment service provider shall adopt and pursue an information security policy defining the general principles and rules to protect the confidentiality, integrity and availability of payment service provider's and its customers' data and information, which shall define in particular the following:

1) information security policy objective and scope;
2) information security management principles;
3) description of main roles, general and specific responsibilities with regard to the information security management.

(2) In its policy referred to in paragraph (1) of this Article, a payment service provider shall define the responsibilities of all employees, contractors and other hired persons with regard to information security, as well as the measures it can take against them in the case of information system security disruption.

(3) A payment service provider shall introduce persons referred to in paragraph (2) of this Article with the information security policy

(4) A payment service provider shall ensure, in its information security policy, confidentiality, integrity, and availability of logical and physical information system resources in accordance with their criticality, and sensitive data whether at rest, in transit or in use.

(5) A payment service provider shall continuously harmonize the information security policy with changes in the information system and its environment, in cases of information system security disruptions, as well as based on the risk assessment results.

(6) A payment service provider shall, based on the information security policy referred to in paragraph (1) of this Article, by way of internal acts prescribe and apply detailed rules relating to all aspects of information security, in particular the following:

1) organisation and governance in accordance with Articles 5 and 12 of this Decision;
2) logical security;
3) physical security;
4) IT operations security;

5) information security monitoring;
6) information security reviews, assessment and testing;
7) information security training and awareness.

(7) A payment service provider providing payment services as a payment institution shall define the policy referred to in paragraph (1) of this Article within the security policy it shall adopt in accordance with the law.

Logical security

Article 14

(1) A payment service provider shall define in its internal acts, and implement the rules for the management of logical access control (identity and access management) which shall ensure at least that:

1) the access to information system is done on a *'need-to-know'* basis, including for remote access;
2) information system users are granted minimum access rights based on their defined business requirements, so that such access rights are minimally required for the uninterrupted execution of their duties;
3) the assigned access rights enable adequate segregation of duties, i.e. the users have not been assigned the combination of access rights that may be used to circumvent controls;
4) where possible, the users are assigned personalised user accounts that ensure that users can be easily identified, and that one account is used by only one user so that the actions performed in the information system could be clearly connected with that user in order to establish user accountability;
5) the use of privileged access rights is strictly controlled by limiting and closely monitoring activities at the account with elevated system access entitlements (e.g. system administrator accounts), and that privileged remote access is granted only on a need-to-know basis and when strong authentication solutions (e.g. two-factor authentication) are used;
6) activities of users and, in particular, all activities by privileged user accounts are recorded in system and operational logs, and that such logs are developed, monitored and retained in accordance with the identified criticality of information system resources referred to in Article 10 of this Decision, for the purpose of timely detection of unauthorised access to and activity in the information system, reconstruction of events and identification of accountability;
7) access rights are granted, withdrawn or modified in a timely manner, according to predefined *approval workflow* that involves the persons identified as responsible for the resources being accessed in accordance with Article 10 paragraph (3) of this Decision;
8) in the case of termination of employment, access rights are promptly withdrawn;
9) access rights are reviewed at least once a year to ensure that users of such rights do not possess excessive privileges and that they are withdrawn when no longer required;
10) authentication methods are applied that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with;
11) the complexity of authentication methods is commensurate with the criticality of IT systems, services, and information being accessed, which, at a minimum,

includes complex passwords or more complex authentication methods, in accordance with risk assessment;

12) access rights for electronic access by IT systems and applications to data and IT systems are limited to a minimum required to provide the relevant service or IT service.

(2) Remote access, within the meaning of this Article, means the access that enables access rights to information system resources from a remote location by using telecommunication infrastructure which is not fully controlled or supervised by the payment service provider.

(3) Privileged access, within the meaning of this Article, means access to information system resources which enables users to have substantially more rights, and to override logical controls (e.g. administrator of system software network, databases, application software, etc.).

(4) Authentication, within the meaning of this Article, means the verification of the identity of the user, system or process by a system.

(5) A payment service provider shall document in more detail the type, content, retention period, security method, frequency of analysis and the method of supervision of operational and system logs being developed in accordance with paragraph (1) of this Article.

Physical security

Article 15

(1) A payment service provider shall in its internal acts, define and implement the physical security controls with the aim to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards (static electricity, high temperature, fire, flood, etc.).

(2) Physical access to IT systems must be monitored and permitted only to the appropriately trained authorised persons, in accordance with their tasks and responsibilities, and physical access to IT systems must be regularly reviewed to ensure, without delay, that unnecessary access rights are promptly revoked when not required.

(3) Adequate measures to protect from environmental hazards must be established in such a manner that they are commensurate with the importance of the buildings and premises and the criticality of the IT systems or operations located in these buildings.

(4) A payment service provider shall periodically review the correctness of physical measures implemented in accordance with this Article.

IT operations security

Article 16

(1) A payment service provider shall, in its internal acts, define and apply rules to prevent the occurrence of security issues in IT systems and IT services and minimise

their adverse impacts on IT service delivery, and these rules shall ensure at a minimum the following:

1) identification of potential vulnerabilities, which shall be evaluated and remediated by ensuring that software components (including firmware and software provided by a payment service provider to its internal and external users) are up to date, by deploying critical security patches or by implementing compensating controls;
2) implementation of secure configuration baselines of all network components;
3) implementation of network segmentation, data loss prevention systems and the encryption of network traffic in accordance with the data classification;
4) protection of endpoints including servers, workstations and mobile devices;
5) the evaluation whether endpoints meet the security standards defined by the payment service providers before they are granted access to the corporate network;
6) application of mechanisms for verifying the integrity of software, firmware and data;
7) encryption of data at rest and in transit in accordance with the data classification.

(2) A payment service provider shall on an ongoing basis, determine whether changes in the existing operational environment influence the existing security measures, require their adjustment, or the adoption of additional measures to mitigate related risks appropriately.

(3) Changes referred to in paragraph (2) of this Article must be carried out in accordance with the formally defined change management process referred to in Article 28 of this Decision.

Information security monitoring

Article 17

(1) A payment service provider shall in its internal acts, define and implement rules for continuous monitoring of information security and detecting unusual events that may impact payment service provider's information security and rules for responding to these events appropriately.

(2) As a part of continuous information security monitoring, a payment service provider shall implement effective measures for detecting physical and logical intrusions as well as breaches of confidentiality, integrity and availability of information.

(3) The continuous information security monitoring process shall include:

1) relevant internal and external factors, including business and IT functions;
2) transactions to detect misuse of access by employees, third parties or other entities;
3) potential internal and external threats.

(4) A payment service provider shall establish and continuously implement controls for detecting events such as undesirable information leakages, presence of malicious software and use of software containing publicly known technical vulnerabilities.

(5) An organisational part and/or persons responsible for monitoring payment service provider's information security shall constantly monitor security and operational threats that could materially affect the ability of a payment service provider to provide services, and monitor technological and security developments to ensure that they are aware of potential risks.

(6) An organisational part and/or persons responsible for monitoring payment service provider's information security shall, in a timely manner, report to a payment service provider’s competent bodies of regular and extraordinary activities with regard to monitoring information security, and, in particular, of detected events that have affected or may affect payment service provider's information security.

Information security testing

Article 18

(1) A payment service provider shall, in its internal acts, define and implement rules for information security testing that validates the robustness and effectiveness of information security measures in place.

(2) A payment service provider shall, in its rules for information security testing referred to in paragraph (1) of this Article, ensure that tests:

1) are carried out by persons who are not involved in the development of the information security measures and who have sufficient knowledge, skills, and experience in testing such measures;
2) include, in accordance with the risk assessment, threat-led penetration testing and scanning of IT systems to detect vulnerabilities.

(3) A payment service provider shall periodically repeat tests of information security measures, at least on an annual basis for all critical IT systems, or at least once in three years for non-critical IT systems.

(4) A payment service provider shall perform extraordinary tests of information security measures when:

1) the infrastructure, and significant processes and procedures change;
2) the changes occur due to significant operational or security incidents;
3) the new or significant changes of the existing critical applications that are available on the Internet are introduced.

(5) A payment service provider shall in its information security testing rules also include the security measures relevant to:

1) payment terminals and devices used for the provision of payment services;
2) payment terminals and devices used for authenticating the payment service users;
3) devices and software provided by the payment service provider to the payment service users to generate/receive authentication codes.

(6) A payment service provider shall, in accordance with the results of the tests referred to in this Article, adjust information security measures, and in case of critical IT systems, it shall do so without delay.

(7) The results of regular and extraordinary information security testing of the payment service provider shall be a part of comprehensive assessment of operational and security risks related to payment services, which the payment service provider shall submit to the Central Bank in accordance with the law.

Information security training and awareness

Article 19

(1) A payment service provider shall, in accordance with current trends, pass, carry out and regularly update the information security awareness programme.

(2) A payment service provider shall in accordance with the programme referred to in paragraph (1) of this Article, at least on annual basis, provide periodical training to all employees and other natural persons hired by a payment service provider, to ensure that they are trained to perform their duties and responsibilities in accordance with information security policy and rules, with the aim to reducing human errors, thefts, frauds, misuses or losses, and be aware how to address payment service provider's information security-related risks.

IT operations management

Article 20

(1) A payment service provider shall manage its IT operations based on formally defined processes that are described in clear, complete and detailed procedures.

(2) A payment service provider shall ensure that performance of their IT operations is aligned to its business requirements, and maintain and improve, when possible, efficiency of their IT system and operations, including the need to consider how to minimise potential errors arising from the execution of manual tasks.

(3) A payment service provider shall maintain and regularly update the list of software and hardware components of information system that contains basic information on their configuration and enables prompt identification of components, their locations, security classification and ownership.

(4) A payment service provider shall regularly maintain documentation which describes interdependencies and links between different software and hardware components of information systems to enable proper configuration and change management and prompt response to security and operational incidents including cyber-attacks.

(5) A payment service provider shall regularly maintain records on all external connection points through which third persons may have unauthorised access to the internal part of information system of a payment service provider, and on all devices which have access to Internet.

Hardware and software asset management

Article 21

(1) A payment service provider shall manage hardware and software assets during its life, form its purchase or development to withdrawal from use, to ensure that it constantly meets business and risk management requirements.

(2) A payment service provider shall, in managing assets referred to in paragraph (1) of this Article, ensure appropriate maintenance of hardware and software assets in accordance with the manufacturer's recommendations, and mitigate risks arising from the outdated assets or from the use of assets that no longer have manufacturer's support.

(3) A payment service provider shall establish and develop IT systems and IT services in the manner that is compliant with business impact analysis results referred to in Article 30 of this Decision, which shall ensure duplication of certain critical components in order to prevent interruptions caused by events affecting those components.

System and operational logs

Article 22

(1) A payment service provider shall develop, monitor and ensure keeping of system and operational logs from critical IT systems, in order to detect, analyse and correct errors.

(2) A payment service provider shall document in more detail the type, content, retention period, security method, frequency of analysis and the method of supervision of operational and system logs being developed in accordance with paragraph (1) of this Article.

Performance and capacity planning and monitoring

Article 23

A payment service provider shall establish a process for planning and monitoring the performance and capacities of IT systems to prevent, detect and respond to important performance issues of these systems and their capacity shortages in a timely manner.

Data backup

Article 24

(1) A payment service provider shall establish the process for managing data backups which includes the process of developing, storing and testing data backups and restoration from backups to ensure availability of data if needed.

(2) The process referred to in paragraph (1) of this Article must be established in accordance with the requirements with regard to recovery or restoration procedures and established criticality of business processes, data, IT systems and IT services, and the implemented risk assessment.

(3) Data backups must be regularly updated, secured and appropriately stored on one or more safe locations, of which at least one must be sufficiently remote from the primary site so they are not exposed to the same risks.

(4) A payment service provider shall identify in its internal act the type, volume, the manner and frequency of development, testing and storing of data in a remote location, storing period for backups and the manner of keeping records thereof.

Incident and problem management

Article 25

(1) A payment service provider shall establish an incident and problem management process to minimise the impact of adverse events and enable prompt and efficient response, and especially in the case of significant operational and security incidents.

(2) A payment service provider shall determine criteria and thresholds for classifying events as operational or security incidents, as well as early warning indicators that will enable early detection of these incidents.

(3) The incident and problem management process shall include:

1) the procedures to identify, track, log, categorise and classify incidents based on priorities, in accordance with the adverse impact they have or might have on operations;
2) the roles and responsibilities for different incident scenarios and categories of incidents;
3) procedures of prompt response to incidents to mitigate adverse impacts of incidents and to ensure that the service becomes operational and secure;
4) procedures for identifying, analysing and solving root causes behind one or more incidents to prevent their recurrence;
5) effective internal communication plans, including communication with regard to incident notification and escalation to higher level of management, and security related payment service users' complaints, to ensure that:
    - all incidents with potentially high adverse impact on critical IT systems and services are reported to the managers of all relevant organisational units in a timely manner;
    - the competent bodies of the payment service provider are informed on an ad hoc basis in the event of significant incidents and, at least, informed of the adverse impact, the response and the additional activities to be taken as a result of the incidents;
6) efficient external communication procedures for critical business functions and processes in order to:
    - collaborate with relevant stakeholders to effectively respond to and recover from the incident;
    - provide timely and appropriate information to clients and other parties in accordance with regulations.

IT project management

Article 26

(1) A payment service provider shall establish the IT project governance process that adequately supports the implementation of information system development strategy referred to in Article 7 of this Decision.

(2) A payment service provider shall establish and implement an IT project management policy to include at least:

1) project objectives;
2) roles and responsibilities;
3) a project risk assessment;
4) a project plan, timeframe and steps;
5) key milestones;
6) change management requirements.

(3) Roles and responsibilities referred to in paragraph (2) item 2) of this Article should be defined so that information security requirements are analysed and approved by an organisational part and/or a person that is independent from the organisational part and/or a person responsible for IT system development.

(4) A payment service provider shall, in its internal acts related to IS risk management referred to in Article 8 of this Decision, appropriately include risks related to IT projects.

(5) A payment service provider shall manage risks arising from the IT project portfolio in an adequate manner (project management), taking into account, in particular, risks that may arise from interdependencies of different projects and dependencies of different projects from the same resources and/or expertise.

(6) A payment service provider shall ensure that all business areas and functions affected by the IT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

(7) A payment service provider shall establish reporting to the payment service provider's competent bodies on regular and ad hoc activities regarding the IT project management, on individual or aggregate basis, depending on the importance and size of the IT project and, in particular, on the launching of the project, its implementation status and associated risks.

IT system acquisition and development

Article 27

(1) A payment service provider shall, in its internal acts using risk-based approach, define and implement rules governing the IT system acquisition, development and maintenance, which shall at least ensure that:

1) before any acquisition or development of IT systems, the functional and non-functional requirements, including information security requirements, are clearly defined and approved by relevant persons;

2) measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the IT systems during development and/or implementation in the production environment;
3) acquired and developed IT systems are tested and approved by applying adequate methodology prior to their first use in production.

(2) In its methodology for testing and approving IT systems, a payment service provider shall ensure that:
1) the identified criticality of business processes and other relevant information system resources has been taken into consideration during the testing process;
2) the testing process confirms the reliability of the new IT system or that such system functions as intended;
3) the testing is performed in the testing environment that adequately reflects the production environment;
4) the implementation of information security measures is tested to identify potential security weaknesses, violations or incidents.

(3) A payment service provider shall separate in an adequate manner development, testing and production environments to ensure segregation of duties, adequate development and testing.

(4) A payment service provider shall restrict the use of production data in development, testing and other non-production environments and ensure the integrity and confidentiality of those data on all systems.

(5) Access right to production data shall be assigned only to authorised users, regardless of the environment of such data.

(6) A payment service provider shall implement measures to protect the integrity of the source program codes of IT systems that are developed in-house.

(7) A payment service provider shall document the development, implementation, operation and/or configuration of IT systems to reduce the risk of dependency on the subject matter professionals/experts.

(8) The documentation referred to in paragraph (7) of this Article should be comprehensive, accurate and regularly updated and, where applicable, it should contain at least user documentation, technical system documentation and operating procedures.

(9) In accordance with risk assessment, the provisions of this Article shall also apply to software solutions developed or managed by internal end users outside the IT organisational unit, such as end user computing applications.

(10) A payment service provider shall maintain records of applications that meet the characteristics listed in paragraph (9) of this Article if they support critical business functions and processes.

Change management

Article 28

(1) A payment service provider shall establish and implement an IT hardware and software components' change management process to ensure that all changes to information systems are assessed, tested, approved, implemented and recorded in a controlled manner and that restoration plans are being established in order to avoid that changes lead to unexpected and unwanted behaviour of this system, i.e. disrupt its security or functionality.

(2) A payment service provider shall ensure that changes of hardware and software components, which, in order to overcome emergencies must be introduced as soon as possible, are implemented in accordance with procedures that provide adequate safeguards.

Business continuity management

Article 29

A payment service provider shall establish business continuity management process to ensure the service provision continuity and limit losses in the event of severe business disruption or interruption.

Business impact analysis

Article 30

(1) As a part of business continuity management process referred to in Article 29 of this Decision, a payment service provider shall periodically analyse its exposure to severe business disruptions and interruptions, and assess their potential business impact, qualitatively and quantitatively, using available internal and external data and scenario analysis.

(2) A payment service provider shall, during business impact analysis referred to in paragraph (1) of this Article, consider the identified classification and interdependency of business functions, processes, information assets, IT systems, IT services, employees and external service providers referred to in Articles 9 and 10 of this Decision.

(3) Based on business impact analysis referred to in paragraph (1) of this Article, a payment service provider shall formally identify:

1) key/critical business activities, processes, IT systems and services, including outsourced activities;
2) service levels a payment service provider is required to maintain or timely restore;
3) recovery time objective (RTO), which indicates the maximum acceptable time within which business process and IT systems and services must be restored after an incident;
4) recovery point objective (RPO), which indicates the maximum time period during which it is acceptable for data to be lost in the event of an incident.

Business continuity planning

Article 31

(1) A payment service provider shall define a *business continuity plan* (BCP) based on the business impact analysis referred to in Article 30 of this Decision.

(2) When defining the business continuity plan referred to in paragraph (1) of this Article, a payment service provider shall coordinate such activities with all relevant internal and external stakeholders and consider dependences from third parties and services they provide.

(3) When defining the business continuity plan referred to in paragraph (1) of this Article, a payment service provider shall consider risks that might have an adverse impact on its objectives with regard to the protection, and if needed, restoration of availability, integrity, and confidentiality of its business functions, supporting processes, IT systems, IT services and information assets.

(4) The business continuity plan referred to in paragraph (1) of this Article must be designed to enable the payment service provider to react appropriately to potential emergency situation scenarios and to recover the operations of its critical business activities after disruptions within a recovery time objective (RTO) and a recovery point objective (RPO).

(5) The business continuity plan referred to in paragraph (1) of this Article must contain a list of priorities to be used in case there is a need to recover several business activities.

(6) A payment service provider shall, in its business continuity plan referred to in paragraph (1) of this Article, consider a range of different scenarios to which it might be exposed, including extreme but plausible scenarios as well as a cyber-attack scenario, and it should describe how the continuity of IT systems and services, as well as the payment service provider's information security, are ensured.

Information system disaster recovery plan

Article 32

(1) A payment service provider shall, considering short-term and long-term recovery objectives, define information system disaster recovery plan(s) based on business impact analysis referred to in Article 30 of this Decision and possible scenarios referred to in Article 31 paragraph (6) of this Decision.

(2) Information system disaster recovery plan referred to in paragraph (1) of this Article shall, in particular, define the following:

1) conditions to be met to implement the plan;
2) a detailed description of procedures that enable recovery and availability of at least key/critical IT systems and services in accordance with defined requirements;
3) a list of priorities to be met if the recovery of more IT systems and/or services is needed;

4) data on teams to be responsible for the recovery of individual IT systems or services, and on team members, including their clearly defined duties and responsibilities;
5) data on the information system recovery location;
6) data on key service providers.

(3) The plan referred to in paragraph (1) of this Article must be directed towards the recovery of operations of critical business functions, processes performed within such functions, information assets and their interdependencies, in order to avoid adverse effects on the functioning of the payment service providers and the financial system, including payment systems and payment service users, and in order to ensure the execution of pending payment transactions.

Testing, updating and availability of plans

Article 33

(1) A payment service provider shall regularly test the plans referred to in Articles 31 and 32 of this Decision and compile reports thereof, where the appropriateness of plans for key/critical business activities, processes, IT systems and services shall be verified at least annually based on extreme, but plausible scenarios.

(2) A payment service provider shall, in the testing process referred to in paragraph (1) of this Article, establish whether it can successfully transfer to an alternative method of performing critical business activities from the disaster recovery environment, maintain such mode for a sufficiently representative period of time and restore normal functioning afterwards.

(3) A payment service provider shall regularly revise and update plans referred to in Articles 31 and 32 of this Decision in accordance with lessons learned from previous incidents, testing results, new identified risks and threats, changed objectives and recovery priorities, business changes, including changes in products, activities, processes and systems, changes in environment and business strategy.

(4) For the purpose of effective implementation of plans referred to in Articles 31 and 32 of this Decision, a payment service provider shall ensure that all employees are aware of their roles and responsibilities in case of contingencies and that these plans are readily available to them in contingencies.

Contingency reporting and communication

Article 34

(1) A payment service provider shall ensure reporting to competent bodies of the payment service provider on activities regarding all relevant facts arising from business continuity management and, in particular, on testing of plans referred to in Articles 31 and 32 of this Decision, analysis of deficiencies identified during the testing process, and significant changes in business continuity management.

(2) A payment service provider shall have measures in place so that, in the event of disruption of business or another emergency, all relevant internal and external stakeholders are informed thereof, and it shall maintain communication with them.

Payment service user relationship management

Article 35

(1) A payment service provider shall establish and implement processes to enhance payment service users' awareness of the security risks linked to the payment services by providing payment service users with assistance and guidance.

(2) A payment service provider shall regularly update the assistance and guidance offered to payment service users in the light of new threats and vulnerabilities, and communicate such changes to the payment service users.

(3) Where product functionality permits, a payment service provider shall allow payment service users to disable specific payment functionalities related to the payment services offered by the payment service provider to the payment service users.

(4) Where a payment service provider has agreed with the payer the spending limits for payment transactions executed through specific payment instruments, the payment service provider shall provide the payer with the option to adjust these limits up to the maximum agreed limit.

(5) A payment service provider shall provide payment service users with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their accounts.

(6) A payment service provider shall keep payment service users informed about updates in security procedures that affect those users.

(7) A payment service provider shall provide payment service users with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services.

(8) A payment service provider shall inform payment service users about how the assistance referred to in paragraph (7) of this Article can be obtained.

III. FINAL PROVISION

Entry into force

Article 36

This decision shall be published in the "Official Gazette of Montenegro", and it shall enter into force on the day of entry into force of the Law Amending the Payment System Law (OGM 111/22).

COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

Decision number: 0101-3480-3/2023
Podgorica, 28 April 2023

CHAIRPERSON
GOVERNOR,

Radoje Žugić, m.p.