INFORMATION SECURITY POLICY AND CYBER SECURITY

It replaces NO-02.05, of 06/28/2005

1. INTRODUCTION

1.1. Information is a property of Cemig and an essential asset to enable the Company to comply with its business purposes and serve society.

1.2. Cemig recognizes the cyber space as an indispensable resource for the execution of its business strategies.

1.3. The cyber security strategy of Cemig is based on the application of best practices to protect the business ecosystem, through a cyber security risk management program.

1.4. This Policy establishes general guidelines, principles and responsibilities to ensure that the information of Cemig and its customers are protected against unauthorized disclosure, modification or access.

2. PURPOSES

2.1. To ensure that information security and cyber security are integrated into all activities and processes of Cemig.

2.2. To manage and reduce information security and cyber security risks, strengthen the image of the Company, comply with business requirements and regulatory and legal requirements.

2.3. To establish processes and implement technologies allowing Cemig to identify, prevent, detect and reduce cyber risk.

3. PRINCIPLES

3.1 Cemig bases its processes and activities on the following principles:

3.1.1 **Operational Security**: the protections implemented must have as their main premise the safeguarding and respect for human life, ensuring that a cyber security or information security incident does not become an accident that can cause damage to the physical integrity of people.

3.1.2 **Availability**: the protections implemented must consider all requirements that maintain the availability of information systems imposed by the business need. No protection measures implemented may compromise availability or affect performance required by the business.

3.1.3 **Integrity**: the protections implemented must guarantee the maintenance of the initial conditions of the information, according to the way in which it was produced and stored.

3.1.4 **Confidentiality**: the protections implemented must be based on the guarantee that the information shall be accessible only to authorized persons.

3.1.5 **Applicability**: the security controls implemented assume a feasible procedure and a structure compatible with the organization of Cemig.

3.1.6 **Monitoring**: the selected security controls must be able to notify any event likely to impact the proper functioning or protection of information systems.

3.1.7 **Traceability**: information systems must have records of actions taken, allowing it to be possible to identify those responsible for them, as well as the exact moment they occurred.

4. APPLICATION

4.1. This Policy applies to all Cemig activities involving employees, third parties, suppliers, consultants, partners and customers, as well as information assets related to the provision of services in cyberspace.

5. TOP MANAGEMENT COMMITMENT

5.1. The Board of Directors, the Presidency and the Executive Board understand the importance of information security and cyber security for Cemig.

5.2. There is a commitment to effective management of actions to identify, mitigate and monitor the risks associated with cyber threats and for this Policy to be properly communicated, understood and followed at all levels of the organization.

6. GUIDELINES

6.1. All information acquired, processed, stored and transmitted is considered to be property of Cemig and must be adequately protected.

6.2. All information owned by Cemig must be used only for the authorized purpose and protected from risks and threats that could compromise its confidentiality, integrity or availability.

6.3. The resources, systems, equipment and services provided for the development of professional activities are the property of Cemig and must be used only for this purpose.

6.4. Access to computerized systems must use systems and technologies authorized by Cemig, through personal and non-transferable credentials and must follow the security criteria defined by the Company.

6.5. Cemig uses rules and procedures in line with this Policy to define protection measures and reach the defined purposes and, once approved, they become an integral part of this Policy.

6.6. Cemig shall monitor and record all activities carried out, using available resources, with the aim of protecting assets and its image, which may be used for administrative and legal purposes, in addition to supporting authorities in case of investigations.

6.7. The information security actions of Cemig must be periodically evaluated, based on the best practices recommended by standards and frameworks, with the aim of raising the level of maturity of the information security process.

7. PROCESSES

7.1. Cemig uses the processes described below to ensure that security controls are implemented and that information and cyber assets have adequate levels of protection:

a. **Asset management**: classification of Information Technology (IT) and Operation Technology (OT) assets, including hardware and software, according to the organization's criticality and purposes.

b. **Vulnerability management**: use of appropriate plans, procedures and technologies to detect, identify, analyze, manage and respond to vulnerabilities and cyber threats.

c. **Cyber risk management**: execution of processes to identify, analyze and respond to cyber risk in the Information Technology (IT) and Operation Technology (OT) environments.

d. **Identity and access management**: creation and management of identities for entities that access the Cemig environment, with access control based on least privilege, business needs and segregation of roles.

e. **Handling security incidents**: use of plans, procedures and technologies to detect, analyze, mitigate, respond to and recover from cyber security incidents and ensure the continuity of operation of services and systems of Cemig.

f. **Monitoring**: activities and technologies to collect, monitor and analyze Information Technology (IT) and Operations Technology (OT) communications to establish the ability to understand the operating environment and the ability to respond quickly.

g. **Risk management in suppliers**: Establishing security controls to manage cyber risk from suppliers and service providers.

h. **Awareness**: plans, technologies and controls used to create a culture of information security and ensure that the workforce can recognize risk situations and act correctly.

i. **Security architecture**: management of processes, controls and technologies to identify security requirements for cyber assets and design appropriate controls to protect them.

j. **Management of the information security program**: establishment of a program that supports the governance, planning and promotion of cyber security activities, aligning security objectives with the organization's purposes.

8. RESPONSIBILITIES

8.1. Information security is the responsibility of each employee, third party, supplier, consultant and partner, each of whom must know and understand the guidelines and principles established

to comply with this Policy and be committed to the adequate protection of information and systems against threats and risks.

8.2. All persons with access to the Cemig environment must participate in awareness-raising activities regarding this Policy, with the aim of mitigating possible security risks, understanding their responsibilities and following the recommended procedures.

8.3. All employees must report any breaches of the Information Security and Cyber Security Policy to the Information Security area.

8.4. The *Leadership* is responsible for guiding everyone under its coordination on the content of this Policy, instructions and other safety guidelines and ensure compliance.

8.5. The Privacy, Data Protection and Cyber Security Committee is responsible for periodically evaluating and monitoring cyber security and information security actions, guaranteeing resources for the execution of activities and supporting actions to promote this Policy.

9. FINAL PROVISIONS

9.1. This Policy shall be updated when any relevant fact or event occurs that motivates its review or according to the analysis and decision of the Privacy, Data Protection and Cyber Security Committee.

9.2. Violations of this Policy and its related documents shall be considered acts of disobedience, subject to the application of direct administrative sanctions and also those provided for in current legislation.

BOARD OF DIRECTORS
*** Policy approved by the Board of Directors on April 18, 2022**