INFORMATION SECURITY AND CYBERSECURITY POLICY

Replaces NO-02.05, dated 28/06/2005

1. INTRODUCTION

1.1 Information is a Cemig asset and an essential resource that enables the Company to achieve its business objectives and serve society.

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

1.3 Cemig's cybersecurity strategy is based on the application of best practices to protect the busi ness ecosystem through a cybersecurity risk management program.

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

2. OBJECTIVES

2.1 Ensure that information security and cybersecurity are integrated into all Cemig activities and processes.

2.2 Manage and reduce information security and cybersecurity risks, strengthen the Company's reputation, and comply with business requirements as well as regulatory and legal obligations.

2.3 Establish processes and implement technologies that enable Cemig to identify, prevent, detect, and mitigate cyber risk.

3. PRINCIPLES

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

3.1.1 **Operational Security**: the protections implemented much have as their primary premise the safeguarding of and respect for human life, ensuring that a cybersecurity or information security incident does not become an accident capable of causing harm to the physical integrity of individuals.

3.1.2 **Availability**: the protections implemented must consider all requirements necessary to maintain the availability of information systems as required by business needs. No protection measure implemented may compromise availability or affect the performance required by the business.

3.1.3 **Integrity:** the protections implemented must ensure the preservation of the original condition of information, according to the manner in which it was created and stored.

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

3.1.5 **Applicability:** the implemented security controls must assume feasible procedures and a structure compatible with Cemig's organization.

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

3.1.7 **Traceability**: information systems must maintain records of actions performed, enabling the identification of those responsible as well as the exact time at which such actions occurred.

4. APPLICATION

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

5. COMMITMENT OF SENIOR MANAGEMENT

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

5.2 There is a commitment to effectively managing actions to identify, mitigate, and monitor risks associated with cyber threats and to ensure that this Policy is properly communicated, understood, and followed at all levels of the organization.

6. GUIDELINES

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

6.2 All information owned by Cemig must be used only for authorized purposes and protected against risks and threats that may compromise its confidentiality, integrity, or availability.

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

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

6.5 Cemig uses standards and procedures aligned with this Policy to define protection measures and achieve the established objectives, and once approved, they become an integral part of this Policy.

6.6 Cemig may monitor and record all activities performed through the available resources for the purpose of protecting its assets and reputation, and such records may be used for administrative and legal purposes, as well as to support authorities in investigations.

6.7 Cemig's information security actions must be periodically evaluated based on best practices established by standards and frameworks, with the purpose of increasing the maturity level 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 Operational Technology (OT) assets, including *hardware* and *software*, according to the organization's criticality and objectives.

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 Information Technology (IT) and Operational Technology (OT) environments.

d. **Identity and Access Managemen**t: creation and management of identities for entities accessing the Cemig environment, with access control based on least privilege, business need, and segregation of duties.

e. **Security Incident Management**: use of plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity incidents and ensure continuity of Cemig's services and systems operations.

f. **Monitoring**: activities and technologies to collect, monitor, and analyze Information Technology (IT) and Operational Technology (OT) communications to establish situational awareness of the operating environment and enable rapid response capabilities.

g. **Supplier Risk Management**: establishment of security controls to manage cyber risk associat ed with suppliers and service providers.

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

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

j. **Information Security Program Management**: establishment of a program that supports governance, planning, and promotion of cybersecurity activities, aligning

security objectives with organizational objectives.

8. RESPONSIBILITIES

8.1 Information security is the responsibility of every employee, third party, supplier, consultant, and partner, and each individual must know and understand the guidelines and principles established for compliance with this Policy and remain committed to the proper protection of information and systems against threats and risks.

9. FINAL PROVISIONS

9.1 This Policy shall be updated whenever any relevant fact or event occurs that motivates its revision or as determined through analysis and decision by the Privacy, Data Protection, and Cybersecurity Committee.

9.2 Violations of this Policy and its related documents shall be considered acts of non-compliance and shall be subject to direct administrative sanctions, as well as those provided for under applicable legislation.

BOARD OF DIRECTORS
*** Policy approved by the Board of Directors on 18/04/2022**