Policy

(PL)

Date of Publication	09/02/2021	Version	01

Origin	Executive Committee (CE) – Approved by OS/21/003

Title: **Cybersecurity Policy**

Document assigned to: ***Cyber Security* Department**

Contents

When printed, this document is an uncontrolled copy

SUMMARY

This policy outlines the requirements and mechanisms to prevent, detect and respond to Cybersecurity risks and threats in ATLANTICO's Information Systems (IS).

1. OBJECTIVE

This policy outlines the guidelines to regulate ATLANTICO security information, in line with the principles contained in its Mission, Vision and Values, with a view to:

a) Contribute to maintaining the trust of clients, employees, shareholders and regulators in ATLANTICO's ability to protect the assets under its responsibility from threats associated with information systems or other types of threats, accidental or intentional, that may compromise its confidentiality, integrity and availability;

b) Comply with legal, regulatory and contractual obligations applicable to ATLANTICO;

c) Detect events that may indicate actions that could compromise ATLANTICO's assets;

d) Provide an effective and efficient response capability in the event of occurrence of information security incidents;

e) Operate ATLANTICO's information systems security strategy, taking into account the current and future challenges, to which ATLANTICO must respond, in line with technological development [e.g. Bring Your Own Device (BYOD)], observing the principles of:

  - **Confidentiality** – ensure that only those who are authorized can access information;;
  - **Integrity** – Ensuring that information and the methods used to handle and process it are precise and compete;
  - **Availability** – ensure that authorized users have access to the information strictly necessary for their work and to the associated assets when they so request.

Thus, it is a legal and ethical obligation of ATLANTICO to guarantee, under the same terms and according to relevant procedures, for the institutions and competent official bodies, strictly necessary information regarding its activity and its clients.

Information created, processed and stored in the internal information systems under these premises, regardless of its form or format, and used during the operative and administrative activities of its business, is considered an asset belonging to ATLANTICO. Included in the previous definition is the information given to ATLANTICO under the established legal scope and that will be considered as its own asset, included in the exclusive assets under its protection.

The various computer resources (hardware, software and licensed products) used to administer, access and manage the information belonging to ATLANTICO shall also be considered as assets to be protected.

2. SCOPE OF APPLICATION

This Policy is applicable to all ATLANTICO employees, interns, partners, consultants and service providers. The requirements for the protection of data and information as set out in this policy must also be observed and complied with by external partners and third parties (including consultants, contractors or service providers) whenever they provide services for, or on behalf of, ATLANTICO.

3. HANDLING OF CYBERSECURITY RISK INFORMATION

ATLANTICO as a whole has the responsibility to identify, assess and manage the broad spectrum of risks to which it is subject, and adopts the "Three Lines of Defense" model to ensure that risks and controls are adequately managed by its processes, people and technology continuously and permanently:

- **First Line** – comprises Business and Support units. Specialized technical teams responsible for installing and operating the Information Technology (IT) environment and a standby cybersecurity team responsible for driving compliance with policies and standards on systems usage, implementation and operationalization of security controls on IT infrastructure and networks;

- **Second Line** - The Operational Risk teams, draft and monitor policies and ensure first line operational compliance and operation. Second line teams also provide subject matter expertise for the development and implementation of controls, tools and projects;

- **Third Line** - Internal auditors provide an independent review of the status of first and second line controls and the interaction between them.

4. PRINCIPLES AND CONTROLS OF INFORMATION SECURITY

Information Security consists of the protection of information and information systems against unauthorized access and misuse, disclosure, disruption, modification or destruction, in order to guarantee their confidentiality, integrity and availability.

This Policy outlines the principles that must be adhered to for the acceptable and proper use of hardware, software, systems, applications, data, facilities and information technology networks, as well as telecommunications equipment, based on information security control requirements and objectives, in order to protect ATLANTICO assets.

4.1 Cybersecurity Training and Awareness

ATLANTICO has a continuous cybersecurity training and awareness program that employs various channels targeted at its employees, service providers and customers, including, content on netPHI and social networks, e-mails and new employee education. A mandatory cybersecurity awareness training for employees is conducted annually, and the results of the training shall be monitored.

4.2 Policies

ATLANTICO uses recommended good international practices through the implementation of policies, standards and guidelines for Cybersecurity risks coverage. The following points are to be addressed in the various policies:

a) Security responsibilities defined;

b) Tests to identify deficiencies or lack of control;

c) Policies for the acceptable handling or use of systems or devices in the Organization;

d) Criteria defined for access control, including:

- Have access only to information needed to perform duties;
- Principle of least privilege;
- Exclusive ID;
- Password complexity;
- Access approvals;
- Process transfers;
- Privileged acess;
- Remote access controls.

e) Software development life cycles for applications, including code review, segregation of activities, web services security review;

f) Control of modification/change of requirements and Disaster Recovery and Business Continuity Plan;

g) Procedures for classification of defined information 5 (five) level information classification system: Public, Internal, Restricted, Confidential and Secret. These terms are mentioned in this document);

h) Well-defined policies and procedures for secure handling, transmission and destruction of information;

i) End-user environment policies, covering data leakage, monitoring of applications which data processing infrastructure is not managed by ATLANTICO, information classification and remote access for teleworking;

j) Control of the technical configurations performed on ATLANTICO's infrastructure, systems and networks;

k) Physical control.

4.3 Risk Management

ATLANTICO applies risk management across lines of defense to identify, report and manage risks across the organization. Information security frameworks at ATLANTICO follow internationally practiced standards for the application of best practices.

Risk assessments are conducted periodically to address changes in information security requirements or institutional risk appetite and/or when significant changes occur. ATLANTICO conducts risk assessments on a variety of assets within the organization. These can be physical assets, people, processes, software and information. For instance: regular information security risk assessments on applications and infrastructure to:

a) Identify, quantify and manage security risks to achieve business targets;
b) Provide a means to identify activities and factors that pose the greatest security threats to ATLANTICO;
c) Ensure that the management of security vulnerabilities is done according to their risk classification and that the controls are proportional to the level of risk discovered;
d) Provide a corporate overview of cybersecurity risks and related contingency plans to develop the cybersecurity strategy;
e) Plan the deployment of resources to areas that offer the greatest risk reduction in customer information.

4.4 Identify and Access Management

Identity and Access Management aims to ensure that the potential addition and/or timely and specific modification of accesses is appropriate to the users' duties and is in line with what is established by the Regulator and guided by policies throughout the life cycle of the supporting controls, which include:

a) Requests for creating, changing, blocking and deleting access, which must strictly abide by the rules established by ATLANTICO;
b) Creation of users must comply with ATLANTICO IS user account naming rule;
c) Assignment of privileged users for the management of ATLANTICO's IS is done according to the duties performed;
d) General, service and application users are created and assigned according to established internal rules and in accordance with an approval process;
e) Authentication to the main information systems is done centrally and access to information is done according to the assigned access profiles, following the access profile assignment procedure defined in ATLANTICO;

   The configuration and management of passwords is done centrally and they shall follow the password parameters defined in the Identity and Access Management Policy of ATLANTICO;

f) The monitoring and review of users and access profiles is done periodically and in a systematic and semi-automatic way, as laid down in the procedure.

4.5 Applications Security

First and Second line of defense technical management teams identify threats, use controls and perform tests including:

a) Software security consulting and risk assessments to ensure that threats to ATLANTICO's software and systems are managed to an acceptable level;
b) Information security risk and technical advice for companies, projects or function initiatives;
c) Define and test security-related controls on systems and applications;
d) Installation and monitoring of application-level controls;
e) Development of minimum security standards.

Security testing, i.e., application intrusion testing (which includes the use of the OWASP framework) and code reviews.

4.6 Security Network

To enable an effective and secure management, ATLANTICO uses several strategically implemented technologies in its entire network:

4.7 *Intrusion Detection and Prevention Systems-IDS and IPS*

ATLANTICO has deployed an intrusion detection and prevention system in its network and infrastructure. These systems are managed by the first line of defense. ATLANTICO'S network and infrastructure is monitored 24/7.

4.8 Wireless Networks Managment

Wireless network infrastructure at ATLANTICO central services and branches is protected using access control, monitoring, encryption and authentication mechanisms and is equipped with resources to protect it against unauthorized wireless access points.

4.9 Internet Access Filters

ATLANTICO employees only have internet access to carry out their duties. Access is filtered according to centrally established rules. Additional management approval is required for any non-standard access and may be subject to additional monitoring.

4.10 Data Loss/Leak Prevention

ATLANTICO's Data Loss / Data Leak Prevention Program is established to reduce exposure to the risk of loss through the application of technical controls and processes, as well as employee education. It includes processes to automatically detect and protect restricted and highly restricted information sent externally by ATLANTICO, which includes emails, file transfers and web uploads. ATLANTICO conducts data monitoring to protect against the risks of theft, accidental loss or deliberate exposure of confidential information.

4.11 Infrastructure Security Testing

Infrastructure security testing is a component of ATLANTICO's technical security analysis and is used to validate the security posture of any technology. Infrastructure intrusion tests are conducted on regularly by internal teams as part of technology enhancement processes . In addition, independent testing by specialized third parties using advanced techniques and the most current industry standards to provide additional assurance. The output of such tests is managed within ATLANTICO's risk management process and framework.

4.12 Encryption

ATLANTICO's data is classified according to its sensitivity to ascertain the level of control required, including, but not limited to, encryption to maintain the confidentiality of information, prevent unauthorized data leakage, or provide integrity checks or digital signatures.

ATLANTICO clearly lays out cryptographic standards that require a series of appropriate figures and password compliances (access codes for encrypted information) to meet specific objectives.

4.13 Workstations and Mobile Devices

ATLANTICO's workstations and laptops, by default, have an antivirus software incorporated into their operating systems, configured to automatically and periodically check files and get updates as soon as they become available.

Desktops / laptops have a unique pre-installed custom format that limits administrative access for users;

All workstations and laptops have a disk encryption solution that prevents data leakage in case of theft;

The use of removable devices is restricted to a limited and pre-identified set of authorized employees and encryption controls are automatically applied to such devices;

Access to ATLANTICO's internal network outside the premises is restricted to authorized devices, which are controlled by remote connectivity.
Mobile devices provided by ATLANTICO are centrally managed by applying policies and controls to limit exposure of information, and also provide encryption capabilities for data in transit or idle and data security features for lost or stolen devices.

4.14 Management of Patches

First-line teams perform checks or receive vulnerability notifications from the product supplier and recommended patch responses. The prioritization for patch implementation in ATLANTICO
is determined by the Vulnerability Management Policy which is based on the framework for vulnerability classification CVSS - Common Vulnerability System Standard.

Patches are tested in a quality environment before implementation in production systems. All patch implementations are managed according to ATLANTICO's information systems acquisition, development, maintenance policy.

Proper governance and oversight is exercised through regular engagement and communication with all areas of ATLANTICO and in accordance with the established structure. Monthly security and operational patch compliance reports are done.

4.15 Remote Work

ATLANTICO supports remote working capabilities when appropriate, necessary and according to the process put in place. Additional controls and guidance for employees and contractors working remotely include, but are not limited to:

a) Awareness of the risks of remote working and disclaimer before remote access is provided;
b) Laptop disk encryption;
c) Use of VPN to connect to the internal infrastructure;
Use of a centralized solution to manage devices that do not belong to ATLANTICO.

4.16 Physical Security

Physical security measures are implemented to prevent unauthorized access to ATLANTICO's facilities, resources or information. These measures are reviewed on a regular basis. Measures implemented by ATLANTICO include, but are not limited to:

a) Physical barriers and security guards;
b) Access control systems and ID cards;
c) Video surveillance systems;
d) Intrusion detection systems.

4.17 Cybersecurity Incident Response

ATLANTICO's cyber security incident management and response plan aims to:

- Coordinate cyber security incident management to ensure that all necessary tasks are completed and avoid duplication;
- Ensure that cyber security incidents are investigated in the shortest possible time;
- Ensure that the risk associated with an incident is properly identified, measured and controlled;
- Ensure that the necessary internal notifications and external reports are done;
- Ensure that all cyber security incidents are monitored for analysis and reported to senior management;

4.18 Information Confidentiality Agreements

ATLANTICO discloses information to third parties only if appropriate controls are taken into account and implemented, as may be applicable, for third party access management, use and storage of ATLANTICO information. Controls may include:

- Agree in advance and in writing (e.g. by signing an NDA) on confidentiality and information security obligations with the third party;

- Conduct proper assessments of the information, how and why it should be disclosed;
- The transfer of information is protected by technical controls, as required by ATLANTICO, to enable third parties to meet our legal responsibilities, obligations and regulatory requirements.

4.19 Service Provider Security Management

ATLANTICO has Service Provider management policies and processes (including: Assessment, identification and selection of service providers and suppliers) associated with contracts entered into with providers. ATLANTICO requires them to observe at least the same level of security, in accordance with internationally recommended policies and standards, covering the legal and regulatory requirements that apply to ATLANTICO's information or systems assigned during the provision of service.

Service providers with access to ATLANTICO infrastructure or information are subject to information security due diligence reviews based on their potential risk to the organization. Specific cybersecurity clauses are included in the terms and conditions of service provider contracts.

5. TERM AND VALIDITY

This Policy is effective as of the date of its publication, and may be updated based on modifications arising from new services, new threats and changes in ATLANTICO's Internal Policy.

Prepared by: Cyber Security Department