NEORIS

Title: NEORIS Information Security and Cybersecurity Policy Abstract

Document Type: Policy Abstract	**ID:** CYB-PO-GLO-11
Functional Area: Information Security	**Issue Date:** Oct-2024
Location: Global	**Effective Date**: Oct-2024
Version: 1.0	

1 Revision History

Version	Date	Author	Revised	Approver	Changes
1.0	Sept, 2022	Daniel Mijares	Sebastian Manzanares Rafael Zamora	Verónica Mancho (CIO) Daniel Ramirez (CISO)	• Creation of abstract based on Information Security and Cybersecurity Policy

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

2 Table of Contents

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

3 Objective

The Objective of this document It is provides an abstract of the Information Security and Cybersecurity Policy, so it is easier knowing its main directives.

4 Scope and applicability

This document is applicable to all NEORIS Corporation, its regions, countries, affiliated companies and their employees, contractors, vendors, consultants, and business partners.

5 Roles and Responsibilities

- Management: Management promote NEORIS policies and shall provide a first level of supervision to employees
- NEORIS Employees Shall obey NEORIS Policies

6 Security Organization

- Information security is the responsibility of every employee. Employees shall adhere to all security policies, procedures and standards.
- Business Owner are responsible for the Information Security of their own process and information assets.
- Commercial Areas and Service Delivery Areas (of each Digital) are responsible for the definition of the level of security and Privacy to include in Services. Service Delivery Areas are responsible for establishing and maintaining the security and Privacy level according to the initial definition. It is recommended that the role of Service Security and Privacy coordinator shall be assigned to ensure compliance.
- The **Information Security Team** is responsibility for managing all NEORIS information security initiatives at Corporate Business Support Level.

7 Assets Classification and Control

- NEORIS areas shall draw up and maintain an inventory of all sensitive information assets.
- Service Delivery areas shall have an inventory of information assets in regards clients or projects.
- All information will be classified using the following categories according to the Information Classification policy:
    a) Non-Business
    b) Public
    c) Internal Use
    d) Confidential
    e) Restricted

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- The asset owner shall review periodically the classification assigned to all sensitive information assets to ensure consistency and validity.
- Information asset labels shall be reviewed by the **Business Owner** at least annually for appropriateness.

8 Personnel Security

- Information Security responsibilities shall be documented in job descriptions.
- NEORIS employees shall sign a Non-Disclosure Agreement as part of their initial terms and conditions of employment.
- Contractors and others Third Parties working for NEORIS or NEORIS Client shall also sign a Non-Disclosure Agreement.
- Terms and conditions of employment shall state: "Compliance with the NEORIS information security policy is mandatory". Any non-compliance with this or any other security policy may result in disciplinary action up to and including immediate discharge from NEORIS, and possible prosecution under applicable local, state and federal laws".
- All NEORIS employees and third-party users shall receive appropriate training and regular updates in information security policies and procedures.
- A **security test** shall be applied to all NEORIS employees, in order to reinforce the awareness of the Security Policy and user responsibilities.
- All suspected activities related to information security violations should be informed to: the **Ethics Commission** to ensure correct, fair treatment for employees who are suspected of committing serious or persistent security breaches and to the **Business Owner**.
- Any employee or third-party users found guilty of any information security violation could lead to be separated of his/her functions.

9 Responding to Security Incidents and Malfunctions

- NEORIS employees or contractors shall report any security incident or potential security incidents immediately to IT Security Tool https://itsecurity.neoris.net, Help Desk or itsecurity@neoris.com.
- Security incidents involving Personal Data will be notified to the Data Privacy Officer, DPO. It is important that the notification take place within the first 24 hours
- There shall be a Cybersecurity Incident Response Plan to manage security incidents
- If a security incident affects the operations of a NEORIS´s client, there shall be a security incident notification to the Client designated point of contact in accordance with contract.
- Service Delivery Areas are responsible to perform the client´s notifications, in accordance with Legal and the Cybersecurity Team professional advice. Service Delivery Areas are responsible to manage security incidents internally on NEORIS Delivery teams in project with clients
- Service Security and Privacy coordinator shall be incorporated to the Cybersecurity response team to provide the insight of the Service, its infrastructure, NEORIS responsibilities and to managed internally any issues with the delivery team.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

10 Physical and Environmental Security

- All NEORIS offices shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
- Departments or areas with additional security requirements shall define secure areas to add security mechanisms to protect their information assets.
- Secure facilities/areas shall be protected and monitored by appropriate controls to ensure an adequate level of security.
- Users should lock their computer screen when they are temporarily away from their desk
- Every employee is responsible to minimize the risk of theft of all NEORIS personal computing resources, devices (e.g., desktops, laptops)
- Employees should not connect their own equipment to NEORIS network or Information facilities. Only cellular phones are allowed in a BYOD scheme if properly enrolled in NEORIS Management

11 Communications and Operations Management

- Operating procedures shall specify the instructions for job execution and shall be annually reviewed by the owner.
- Changes Management process shall be established to govern the changes to technology infrastructure.
- Duties and areas of responsibility must be separated to minimize the risk of fraud and errors in the processing of information, transactions or information or services.
- Business Owners are responsible to establish proper Segregation of Duties.
- Prior to using external Facilities Management services, risks shall be identified and appropriate controls agreed with the contractor and incorporated into the contract.
- Capacity planning for critical all information processing systems and information assets shall be performed annually.
- New systems shall be prevented from entering the production environment until system owners have reviewed and authorized the results of acceptance test
- Each end user equipment shall have the authorized virus scanning software. This shall be update automatically.
- Vulnerability scans shall be performed regularly at least one for each quarter, monthly scans are highly recommended.
- Backup copies of critical business information and software shall be taken regularly
- Automate generated logs shall keep system activity.
- Users in remote locations shall use a Virtual Private Network (VPN) and MFA Authentication to safeguard confidentiality and integrity of data passing over public networks.
- NEORIS Network Access shall be protected by Network Access Control who only permit the access to authorized devices and user in compliance with security controls.
- Storing sensitive information in removable media is forbidden for normal users. Only IT personnel in the development of their administrative duties can store sensitive information in removable media.
- E-mail will be used for NEORIS authorized purposes
- E-mail messages are the property of NEORIS
- Only NEORIS official Wireless LAN network shall be used at NEORIS Offices.
- For remote access from public wireless access point a VPN shall be used.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- Employees shall protect the exchange of information using only the official NEORIS managed communications
- Employees shall not discuss confidential information in public areas, public transportation.
- The use of speaker phone to discussed confidential information is restricted to closed areas
- Documents from printers or copiers shall be removed promptly, and never left unattended in the trays.

12 Access control

- Access to NEORIS systems must be provided by MFA Multi-Factor Authentication.
- Unique User ID per user shall be established so user's activities could be traced.
- Users shall be forced to change password at the initial logon to make sure of the confidentiality of the password.
- Password must be changed every 60 days in accordance to NEORIS Password Policy.
- User's access rights shall be reviewed by **Business Owner** at least every 6 months.
- Unattended equipment shall be physical and logical locked. i.e screen lock, log off sessions.
- NEORIS Network Access shall be protected by Network Access Controls who only permit the access to authorized devices and user in compliance with security controls.
- Only NEORIS Owned end user devices, and third parties authorized devices are allowed in NEORIS Infrastructure.
- Access to information and application systems shall be restricted to authorized users in accordance with Business Owner requirements
- Privileged Access Management is required for NEORIS critical corporate system´s information infrastructure
- SIEM Technologies shall be used to further protect NEORIS Infrastructure

13 System Development and Maintenance

- A Secure Software Development Process shall be implemented for NEORIS Clients and internal developments.
- Privacy and security requirements analysis shall be performed when developing Information Systems.
- Worthiness of information security requirements and Privacy shall be resolved by the Business Owner and the Project Security Architect.
- Static and Dynamic Security validation codes shall be done, and the deficiencies resolved prior to system deployment in production environment.
- Strong encryption shall be used to protect communications and highly sensitive information such as personally identifiable information.

14 Business Continuity Management

- Continuity plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.
- For all Catastrophic Scenarios that required Risk Treatment, it shall be stablished Continuity recovery strategies.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global

- Business continuity plans shall be tested once a year or whenever a major change has occurred to ensure that they are up to date and effective.

15 Compliance

- Legal Department shall advise NEORIS on all regulatory requirements regarding information security and privacy to ensure that there is no conflict between the legislation in each country and the information security directives defined in this Policy.
- All employees shall sign the "Non-Disclosure Agreement and Intellectual Property Rights" as part of the hiring process.
- All Consultants and third parties shall sign the "Confidentiality Agreement and Intellectual Property Rights" before working for NEORIS.
- All workstations used for NEORIS business purposes shall be provided with licensed software.
- Software licenses of all software products shall be controlled and maintained by Information Technology Department.
- **Human Resources** remains committed to protecting the privacy and confidentiality of information about its Employees. Establishing uniform practices for collecting, using, disclosing, storing, accessing, transferring or otherwise processing.

16 Information Security Risk Management

- Information Security Risk Management applies to the entire NEORIS infrastructure and business processes. Business Process Owners are accountable for the risk assessment of their own business process.
- Service Delivery Areas shall perform an information security risk assessment if it is mandated by its own processes, it is of part of the service engagement or contract with Client.
- IT Security Team shall perform risk assessments on corporate Infrastructure as well as in the scope of the Information Security and Privacy Management System, ISPMS.

17 Cloud Security

- A specific Cloud Security policy shall be defined and communicated to establish the bases for a proper cloud security framework.
- All NEORIS technical areas such as IT, and all the Digitals are required to comply with the Cloud Security Policy as well as Process Owner and Service Owner that use Cloud.
- NEORIS can use a cloud system, but it must always have evidence of the security of the Cloud Service. Example of this evidence could be ISO Certificates 27001, ISO27701, SOC Type Reports, contracts, among others.

www.neoris.com
1395 Brickel Avenue, Suite 500
Miami, FL 33131, EE.UU.

/neoris
/neoris.corporate
/company/neoris
/neoris_global