NEORIS

Title: Information Security Policy for Contractors

Document Type: Policy	**ID:** CYB-PO-GLO-TdP-12
Functional Area: Information Security	**Issue Date:** Sep-2024
Location: Global	**Effective Date**: Oct-2024
Version: 1.0	

1 Revision History

Version	Date	Author	Revised	Approver	Changes
Version 1.0	Sep 2024	Jesica Maravillas	Rafael Zamora Daniel Mijares Katia Morales	Daniel Ramirez (CISO) Verónica Mancho (CIO) Juliana Fernandez (COO)	• Conversion of security requirements document to Information Security Policy for Contractors • Same requirements, no substantive changes.

2 Table of Contents

3 Objective

The objective of this Policy is to describe the minimum mandatory guidelines that NEORIS Contractors must comply with regarding Information Security.

4 Scope and Applicability

This policy is applicable to all NEORIS Contractors.

5 Roles and Responsibilities

- Supplier Administration (Vendor) must ensure that it communicates and manages the signing of the guidelines contained in the Information Security Policy for Contractors.
- Contractors must comply with the guidelines contained in the Information Security Policy for Contractors.

6 Security in Computer security

In relation to Computer Equipment Owned by the Contractor Company with Access to the NEORIS Network or Clients Network or to Non-public Information services of NEORIS, or NEORIS Clients, the Contractor Company undertakes to comply with and adhere to the following points:

Provide computer equipment to its employees assigned to NEORIS or NEORIS Clients, with the hardware and software requirements established by IT to ensure its proper operation in NEORIS facilities (See Contractor Computer Equipment Specifications Section). Unless there is a contractual agreement that establishes that NEORIS provides the computer equipment to employees of the Contractor Company.

Ensure that all employees assigned to NEORIS have computer equipment owned by the Contractor Company to perform their duties. Except for equipment provided by NEORIS.

The Contractor Company undertakes to avoid at all times the use of computer equipment owned by third parties to perform the services, such as computer equipment owned by employees of the Contractor Companies.

Ensure that your computer equipment complies at all times with:

- The hardware and software requirements established by IT to ensure its proper operation in NEORIS facilities (See Specifications in the Contractor Computer Equipment Section).
- The security configuration established by NEORIS (See Specifications in the Contractor Computer Equipment Section).
- Have the Software, its corresponding license and maintain the Software in support.
- Exceptions in licensing must be authorized by NEORIS Finance, which will indicate the procedure to follow in the event of authorizing the software installation exception by NEORIS.

The Entry and Exit of the computer equipment owned by the Contractor Company must at all times comply with the entry and exit procedure for equipment established in the building where it assists to provide its services, whether for NEORIS or for a NEORIS Client.

Present the computer equipment to the local IT technical support staff to certify that it meets the requirements established in this document.

The Local IT support area will configure the Contractor's computer equipment in accordance with the guidelines required by NEORIS, for which they must have the following characteristics:

- The user must have administrator permissions on the equipment.
- Not have Internet Information Services (IIS) and Indexing Service installed, unless previously authorized in writing by IT.
- For the acceptance of the equipment, the IT area can install agents on the equipment of the external personnel for monitoring. Likewise, the use of network resources by the external user is subject to the Computer Equipment Assignment and Use Policy (IT-PO-GLO-USER-HW-ASS&USE) that is active.
- The user must have a security lock or device with similar functionality which he must use during his stay at the NEORIS or assigned Client facilities.
- The user must have a headset or device with similar functionality to be able to carry out video conference sessions or telephone calls from his equipment.
- External Personnel will only connect to the NEORIS or Client network, either with NEORIS computer equipment or with computer equipment owned by the Contractor Company that has met the NEORIS requirements. Connections to the NEORIS or Clients network from any other machine are strictly prohibited.
- For computer equipment of the Contractor Company that is directly under the administration and security controls of the Client, they must comply with the Client's requirements. This applies whether it is located directly on-site at the Client's facilities or connected remotely via IPSec VPN from the Contractor Company's facilities.
- All computer equipment owned by Contractor Companies that is going to be connected to the NEORIS Network will be subject to NEORIS Security controls, for which the equipment will be entered into the NEORIS domain and will be subject to the security policies established by NEORIS.
- It is the Contractor Company's responsibility to verify that any authorized software that needs to be installed on its equipment does not affect the proper functioning of the equipment. Likewise, it must have the corresponding license that legitimizes its use.

IT will only support those applications owned by NEORIS installed on the equipment. Any support for HW and/or SW owned by the Contractor Company must be provided by the Contractor Company.

In the event that the equipment is being used for a client project outside of NEORIS's facilities, the Contractor Company participating in the execution of said project must comply with the requirements that the Client and the project require it to comply with on its device in order to grant it access. In any case, the Contractor Company assumes as its own the information security commitments signed by NEORIS with the Client and is fully responsible for their compliance.

7 Responsibilities of external personnel users

External users agree to use the NEORIS network or the network of the client to which they are assigned only for the purposes of the contracted service, and any unauthorized commercial and/or private use is prohibited.

External users agree to use good security practices, including but not limited to:

- Make sure you have:
  - Licensed, supported and updated operating system with the latest version and the latest patches installed.
  - Antivirus updated both in its engine and in its malware signatures. Configured for automatic updates. External users must have one of the antiviruses authorized by NEORIS installed on their computers, see appendix A "List of Antiviruses".
  - Automatic blocking of screen saver after 5 minutes of inactivity.
  - Use Strong Passwords of at least 8 characters in length, made up of at least 3 of the following 4 groups:
    - Uppercase letters (A, B, C, D ...).
    - Lowercase letters (a, b, c, d ...).
    - Numbers (0, 1, 2, 3, 4 ...).
    - Special characters (#, $, %, &...).
  - Passwords must be changed at regular intervals of no more than 60 calendar days.
  - Automatic screen lock in case of 5 consecutive password failures.

- Keep your Desk and Screens Clean of Confidential Information when not present.
- External users must validate at least once a week the technical compliance with the provisions of this document and act accordingly to ensure compliance in case they detect any failure, for example, they find that the operating system is not updated, so they must update it to correct it.

The use of computing and network resources by the external user falls under the Computer Equipment Allocation and Use Policy (IT-PO-GLO-USER-HW-ASS&USE) and the following actions are considered prohibited:

- Interfering with the security and protection mechanisms of computer equipment.
- Browsing the Internet anonymously.
- Using information interception software, information discovery such as network scanner, sniffer, etc.
- Sharing software or receiving software without complying with the corresponding licensing.
- Sharing passwords, these must be kept confidential and changed regularly, maximum every 60 calendar days.
- Trying to obtain unauthorized access.
- Copying information to which you do not have access and authorized copying rights.
- Storing information in unauthorized public repositories such as Cloud Drive, personal One Drive, etc. SharePoint Forums or others designated in writing in the project are the only ones authorized as information repositories.
- Using information or computer resources in violation of the policies of NEORIS or its Clients.

- Infringing any damage or interference with the facilities, resources or business processes of NEORIS or its Clients.
- It is strictly prohibited to extract information from NEORIS or NEORIS Clients via USB or any other means.

8 Termination of external personnel (Contractors)

The IT department will cancel access to NEORIS network resources when notification is received from Vendor Administration, who will notify the account termination.

In the event that the employee of the Contracting Company (External Personnel) ends his assignment to NEORIS, or ends his employment relationship with his corresponding Contracting Company, he must go to the IT area to return the equipment to its initial conditions when he entered, removing the licensing installed by NEORIS if there was one, as well as the information through a secure deletion of the information of NEORIS and/or NEORIS Clients. In the event that the Equipment is the property of NEORIS, it must be returned.

9 Information Security Awareness

The Contractor Company undertakes to ensure that all its employees, especially those assigned to NEORIS, are aware of Information Security matters.

The Security Program must include Information Security Awareness Campaigns for its employees. At least the following topics must be covered: Clean Desktop of Confidential Information, Confidentiality and Robustness of Passwords, Safe Browsing, Securing Laptop Computers, Information Security Incidents and their reporting, among others.

All Contractor employees must have a successful annual awareness training. NEORIS may provide sample background material if required.

Contractor Employees assigned to NEORIS must take the Information Security awareness training provided by NEORIS if necessary.

10 Information Technology Incidents

Contractor Company employees assigned to NEORIS must report Information Technology incidents to the NEORIS Help Desk using one of the following mechanisms:

- WhatsApp: +52 81 8888 5910
- MS TEAMS: NEORIS Help Desk
- Email: help.desk@neoris.com
- Extension 5911 (Commutator + Ext 5911)
- WeCare tool: https://wecare.neoris.net/

Office	Commutator	Office	Commutator
Miami	+ 1 305 728 6000	Santiago de Chile	+56 2 2829 7700
Monterrey	+52 81 8888 5000	Buenos Aires	+54 11 4105 7900
Culiacan	+52 81 8888 5000	Rosario	+54 341 512 7400
Mexico City	+52 55 5999 6700	Lima	+51 1 686 6719
Queretaro	+52 81 8888 5000	Madrid	+34 912 11 23 00
Bogota	+57 1 653 0990		
Sao Paulo	+55 11 4134 5700		

- If you require Local Support, please contact:

Region	Name	Email	Phone
Global	Help Desk	helpdesk@neoris.com	Ext. 5911
Rosario Arg.	Sebastian Manzanares	sebastian.manzanares@neoris.com	+ 54 34 1308 0034
Monterrey Mex.	Rafael Zamora	rafael.zamora@neoris.com	+ 52 81 1600 1724
Madrid Esp.	NEORIS Spain IT	it.spain@neoris.com	Ext. 2222

11 Information security incidents

The Contractor Company must report to the Project Manager any security incident in its network infrastructure, information systems and central or user computing equipment that could endanger the computing equipment or information of its employees assigned to NEORIS, NEORIS itself, NEORIS Clients or the information provided in the course of performing the service with NEORIS. The Project Manager will report it to the NEORIS IT security team through http://itsecurity.neoris.net/ or itsecurity@neoris.com.

The Contractor Company agrees to work in good faith to establish containment measures and avoid or at least mitigate potential infections from malicious software.

Contractor Company employees assigned to NEORIS must also report directly and immediately to NEORIS any security incident or suspected incident to:

- WhatsApp: +52 81 8888 5910
- MS TEAMS: NEORIS Help Desk
- ITSecurity http://itsecurity.neoris.net/
- Email: help.desk@neoris.com, or itsecurity@neoris.com
- Extension 5911 (Commutator + Ext 5911)
- WeCare: https://wecare.neoris.net/

Security Incidents with Personal Data. In the event of any security incident involving personal data of one or more individuals, whether due to loss or theft of a laptop, data leak, loss of physical documents, among other situations, the report must indicate that personal data is involved by filling out the Report of Theft or Loss of Computer Equipment form and immediately notifying NEORIS through the established means:

- WhatsApp: +52 81 8888 5910
- MS TEAMS: NEORIS Help Desk
- ITSecurity http://itsecurity.neoris.net/ or itsecurity@neoris.com
- Email: help.desk@neoris.com
- Extension 5911 (Commutator + Ext 5911)

The NEORIS Data Protection Officer (DPO) must receive the report and information within a period of **no more than 24 hours** to carry out an analysis of the situation.

The NEORIS DPO will report these incidents to the corresponding authority within a period of **no more than 72 hours** if applicable.

12 Reporting and compliance

If required by NEORIS, the Contractor Company must provide safety compliance reports with the frequency indicated by NEORIS, which include what is indicated by NEORIS, such as:

a) Inventory of your computer equipment assigned to your employees assigned to NEORIS or NEORIS Clients.
b) Conditions of the Computer Equipment assigned to the provision of the service with NEORIS in relation to this document.
c) Conditions of your Employees assigned to NEORIS projects in relation to this document.

NEORIS reserves the right to establish automatic technical validation mechanisms for compliance, for example, technical validation when connecting to NEORIS VPN remote access.

The Contractor Company acknowledges that its consultants assigned to NEORIS must connect to the timecard tool, for which they will need to connect via remote access to the NEORIS VPN, which, as a requirement for granting access, will perform the basic technical validation of the Operating System and Antivirus update, granting access only to those computers in compliance.

13 Right to audit

The Contractor grants NEORIS the right to audit compliance with the provisions of this document.

The Contractor shall allow NEORIS access to its facilities and computer equipment to conduct a systems audit in accordance with the provisions of this document. The systems audit shall be conducted by

NEORIS or by an inspection body, composed of independent members with the necessary professional qualifications and subject to confidentiality, selected by NEORIS.

The Contractor grants NEORIS permission to install Software to monitor compliance with the security controls stipulated in this document.

14 Contractor´s Computer Equipment Specifications

The minimum acceptable conditions for accepting computer equipment in NEORIS for projects by External Personnel or Contracting Companies are detailed below.

The Contracting Company recognizes that there may be projects that require definitions greater than those specified here, which must be communicated and accepted by the Contractor. The higher definitions must be delivered to the Contracting Company through official Channels.

15 Hardware

- CPU i7 processor or higher preferred*.
- CPU i5 processor acceptable unless otherwise agreed by the client**.
- 512 GB SSD hard drive or higher, preferred*
- 256 GB hard drive or higher acceptable unless otherwise agreed by the client**.
- 16 GB RAM or higher.
- 10/100 Mbps network card.
- Dualband WiFi card.
- Network cable.
- Security lock or similar device.

* It is recommended that all new equipment from the Contractor Company meet the specifications indicated as preferable, since in the future they will be mandatory requirements of NEORIS.
**The Contractor Companies recognize that NEORIS has Clients with higher specifications, and are not eligible to participate in projects with these requirements.

16 Software

For Contractor equipment, the following elements must be installed:

- Microsoft Windows 10 Professional license or later in its latest version (build) available with the following features:
  – English version.
  – Latest patches installed.

- Microsoft Office 2016 or O365 license.
  – In its latest version (build) available.
  – Latest patches installed.

- Controllers and Drivers necessary for the operation of the equipment.
- Additional software required by project and agreed with the Contractor Company.
- Exceptions in licensing must be authorized by NEORIS Finance, an area that will indicate the procedure to follow in case of authorizing the software installation exception by NEORIS.

17 Required Security settings

For the Contractor's computer equipment, the standard defined for operation in NEORIS is the following in terms of security configuration:

- Boot password configured and activated.
- Hard disk password activated.
- Hard disk encryption used BitLocker (Windows computers) or equivalent.
- Screen saver password configured and activated at most every 5 minutes.
- Weekly automatic validation of Operating System and Office Security updates.
- Updated Anti-Malware (Antivirus) protection. The Antivirus must meet the following requirements:
  – Always be installed and activated.
  – Keep updated both in the analysis engine and in the signature database, maximum one week old (in the signature database) and one month in the analysis engine.
  – Automatic antivirus scanning at least once a week.
- Security lock or equivalent in the case of portable computer equipment.
- USB port blocking, Bluetooth for information transfer.

18 Exceptions

Any exceptions to compliance with this Policy must be authorized by NEORIS, any non-compliance that is not justified and approved will be sufficient reason for the cancellation of the contract with the Contractor Company.

The latest version of the document is available on the NEORIS portal.

Annex A “List of authorized Antivirus”

- 360.CN
- adaware
- Agnitum Ltd.
- AhnLab, Inc.
- ALLIT Service, LLC.
- Antiy Labs
- Anvisoft Inc.
- Apple Inc.
- Arcabit
- Ashampoo GmbH & Co. KG
- AsiaInfo, Inc.
- Auslogics
- Avanquest Software
- AVAST Software a.s.
- Avetix S.r.l
- AVG Technologies CZ, s.r.o.
- Avira GmbH
- AxBx
- Baidu Inc.
- Beijing Jiangmin New Sci. & Tech. Co., Ltd
- Beijing Rising Information Technology Co., Ltd.
- BeyondTrust, Inc.
- Bitdefender
- Biz Secure Labs, Pvt. Ltd.
- Bkav Corporation
- BrightFort LLC
- BullGuard Ltd.
- CA, Inc.
- Carbon Black, Inc.
- Check Point Software Technologies
- Chili Security
- Cisco Systems, Inc.
- CJSC Returnil Software
- ClamWin Pty Ltd
- Clearsight Technologies Ltd.
- CMC InfoSec
- Comodo Group
- COMODO Security Solutions
- CrowdStrike, Inc.
- Cybereason
- Cylance Inc.
- Datalink Industrial Corporation
- Defender Pro
- digital-defender
- Doctor Web, Ltd.
- EarthLink, Inc.
- eBilge Teknoloji Sanayi ve Ticaret Anonim Şirketi
- eEye Digital Security
- EGSoftWeb

- Emsisoft Ltd
- Endgame, Inc.
- enSilo
- ePCheal Antivirus
- ESET
- Essentware S.A.
- ESTsoft Corp.
- F-Secure Corporation
- Faronics Corporation
- Filseclab Corporation
- FireEye, Inc.
- Fortinet Inc.
- FRISK Software International
- Fujitsu Services Ltd.
- G Data Software AG
- GEN-X Technologies
- GFI Software Ltd.
- Glarysoft Ltd
- GridinSoft LLC.
- Hauri, Inc.
- HDD Labs. Inc
- Heimdal Security
- idoosoft
- IKARUS Security Software GmbH
- INCA Internet Co., Ltd.
- Intego
- IObit
- iolo technologies, LLC
- Ivanti, Inc.
- K7 Computing Pvt Ltd
- Kapha Anti-Malware, Inc.
- Kaspersky Lab
- Kenoxis
- Kingsoft Corporation
- Komal Technologies.
- Kromtech
- LANDESK Software, Inc.
- Lavasoft
- LogicNow, Inc
- LogMeIn, Inc.
- Lumension Security, Inc.
- MacPaw Inc.
- Malwarebytes Corporation
- Max Secure Software
- Maya Software Technologies
- McAfee, Inc.
- Mega HighTech S.L.
- Microminder
- Microsoft Corporation
- MicroWorld Technologies Inc.
- MINUSOFT INDIA PRIVATE LIMITED
- MSecure Data Labs

- N-able Technologies Inc
- NANO Security
- Nerdy Nynjas
- NETGATE Technologies s.r.o.
- NictaTech Software
- NIFTY Corporation
- NinjaRMM LLC
- Norman AS
- nProtect, Inc.
- Palo Alto Networks, Inc.
- Panda Security, S.L.
- ParetoLogic, Inc.
- PC Cleaners Inc.
- PC Security Shield
- PC Tools Software
- Proland Software
- Qihu 360 Software Co., Ltd.
- Quick Guard Technologies
- Quick Heal Technologies (P) Ltd.
- Radialpoint Inc.
- Reason Software Company Inc.
- REVE Systems
- Roboscan Inc
- Rogers
- Safer-Networking Ltd.
- Scandium Security Inc.
- SecureAge Technology
- SecureHunter, LLC.
- SecureMac.com, Inc.
- Security Software Limited
- SentinelOne
- SGA SOLUTIONS
- ShieldApps
- Smadsoft
- Smart Heal
- SolarWinds Worldwide, LLC.
- SonicWALL L.L.C.
- Sophos Limited
- Sourcefire, Inc
- SOURCENEXT CORPORATION
- SPAMfighter ApS
- SparkTrust
- Stormshield
- SUPERAntiSpyware
- Swiss security laboratory.
- Symantec Corporation
- Systweak Inc.
- TeamViewer GmbH
- Tech Guard Technologies
- TEHTRI-Security
- Telefónica S.A.
- TELUS

- Tencent
- TG Soft S.a.s.
- Thirtyseven4
- ThreatTrack Security, Inc.
- Total Defense, Inc.
- Trend Micro, Inc.
- Trusteer Ltd.
- TrustPort, a.s.
- Unistal Systems Pvt. Ltd.
- VirusBlokAda Ltd.
- WARDWIZ
- Webroot Software, Inc.
- Zemana Ltd.