PETROBRAS	TECHNICAL SPECIFICATION	N°: I-ET-3010.00-5520-800-P4X-005	
	CLIENT:		SHEET: 1 of 9
	JOB:		
	AREA:		
	TITLE: CYBERSECURITY MINIMUM REQUIREMENTS		INTERNAL / ESUP

MICROSOFT WORD / MICROSOFT 365 V.2024 / I-ET-3010.00-5520-800-P4X-005_0.DOCX

INDEX OF REVISION

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL ISSUE

	REV. 0					
DATE	MAY/31/24					
EXECUTION	U5D6					
CHECK	U361					
APPROVAL	CDC1					

SUMMARY

1 INTRODUCTION

1.1 Objective

1.1.1 The objective of this specification is to define the Cybersecurity Minimum Requirements that shall be attended in the design of this UNIT.

1.1.2 These requirements are valid both for Leased units and for Petrobras Owned and Operated Units.

1.1.3 Despite the current definitions for the minimum requirements, every design is welcomed to implement higher security levels and more requirements than stated in this document.

1.2 Abbreviations, Acronyms and Initialisms

DoS	Denial of Service
FAT	Factory Acceptancy Test
FR	Foundational Requirements
OT	Operational Technology
RE	Requirement Enhancements
SAT	Site Acceptancy Test
SIEM	Security Information and Event Management
SR	System Requirements

2 REFERENCE DOCUMENTS, CODES AND STANDARDS

2.1 IEC – International Electrotechnical Commission

- IEC 62443 SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS.

2.2 Brazilian Codes and Standards

All Applicable Brazilian Standards and Codes.

2.3 Project Documentation

2.3.1 Names below and respective document codes may vary according to each project but, in general, the following documents shall be considered along with this technical specification.

2.3.1.1 Any requirements shown in these documents shall also be fully attended to (i.e., requirements presented in these documents are additional requirements). In case of conflict between the requirements of these documents against this document, PETROBRAS shall be consulted.

2.3.1.2 For Petrobras Owned units:

- AUTOMATION AND CONTROL ARCHITECTURE
- AUTOMATION NETWORK DESCRIPTION
- NETWORK INTERCONNECTION DIAGRAM

2.3.1.3 For leased units:

- General Technical Description

3 CYBERSECURITY MINIMUM REQUIREMENTS

3.1 General

3.1.1 CONTRACTOR shall implement a patch management program in accordance with IEC 62443-2-3;

3.1.2 CONTRACTOR shall implement a vulnerability management process in accordance with IEC 62443-3-2 and IEC 62443-2-1;

3.1.3 CONTRACTOR shall implement an incident response process in accordance with IEC 62443-2-1 (Table 17 – Incident planning and response: Requirements);

3.1.4 CONTRACTOR shall communicate to Petrobras any cyber security incident on OT environment and any change or discontinuity in cyber security requirements;

3.1.5 CONTRACTOR shall perform one workshop to address cybersecurity requirements. The agenda and topics to be addressed on these workshops shall be mutually agreed between CONTRACTOR and PETROBRAS. The actions and outcomes from these workshops shall be shared with Petrobras.

3.2 FR 1 – Identification and authentication control

3.2.1 Human user identification and authentication (SR 1.1 - IEC 62443-3-3):

3.2.1.1 The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

3.2.2 Multifactor authentication for untrusted networks (SR 1.1 RE 2 - IEC 62443-3-3)

3.2.2.1 The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).

3.2.3 Account management (SR 1.3 - IEC 62443-3-3)

3.2.3.1 The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

3.2.4 Identifier management (SR 1.4 - IEC 62443-3-3)

3.2.4.1 The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.

3.2.5 Authenticator management (SR 1.5 - IEC 62443-3-3)

3.2.5.1 The control system shall provide the capability to:

- initialize authenticator content;
- change all default authenticators upon control system installation;
- change/refresh all authenticators; and
- protect all authenticators from unauthorized disclosure and modification when stored and transmitted.

3.2.6 Wireless access management (SR 1.6 - IEC 62443-3-3)

3.2.6.1 The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

3.2.7 Strength of password-based authentication (SR 1.7 - IEC 62443-3-3)

3.2.7.1 For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

3.2.8 Authenticator feedback (SR 1.10 - IEC 62443-3-3)

3.2.8.1 The control system shall provide the capability to obscure feedback of authentication information during the authentication process.

3.2.9 Unsuccessful login attempts (SR 1.11 - IEC 62443-3-3)

3.2.9.1 The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.

3.2.9.2 For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

3.2.10 System use notification (SR 1.12 - IEC 62443-3-3)

3.2.10.1 The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

3.2.11 Access via untrusted networks (SR 1.13 - IEC 62443-3-3)

3.2.11.1 The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

3.3 FR 2 – Use control

3.3.1 Authorization enforcement (SR 2.1 - IEC 62443-3-3)

3.3.1.1 On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

3.3.2 Wireless use control (SR 2.2 - IEC 62443-3-3)

3.3.2.1 The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.

3.3.3 Use control for portable and mobile devices (SR 2.3 - IEC 62443-3-3)

3.3.3.1 The control system shall provide the capability to automatically enforce configurable usage restrictions that include:

- preventing the use of portable and mobile devices;
- requiring context specific authorization; and
- restricting code and data transfer to/from portable and mobile devices.

3.3.4 Mobile code (SR 2.4 - IEC 62443-3-3)

3.3.4.1 The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include:

- preventing the execution of mobile code;
- requiring proper authentication and authorization for origin of the code;
- restricting mobile code transfer to/from the control system; and
- monitoring the use of mobile code.

3.3.5 Session lock (SR 2.5 - IEC 62443-3-3)

3.3.5.1 The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.

3.3.6 Auditable events (SR 2.8 - IEC 62443-3-3)

3.3.6.1 The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

3.3.7 Audit storage capacity (SR 2.9 - IEC 62443-3-3)

3.3.7.1 The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

3.3.8 Response to audit processing failures (SR 2.10 - IEC 62443-3-3)

3.3.8.1 The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

3.4 FR 3 – System Integrity

3.4.1 Communication integrity (SR 3.1 - IEC 62443-3-3)

3.4.1.1 The control system shall provide the capability to protect the integrity of transmitted information.

3.4.2 Malicious code protection (SR 3.2 - IEC 62443-3-3)

3.4.2.1 The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

3.4.3 Central management and reporting for malicious code protection (SR 3.2 RE 2 - IEC 62443-3-3)

3.4.3.1 The control system shall provide the capability to manage malicious code protection mechanisms.

NOTE: Such mechanisms are commonly provided by endpoint infrastructure centralized management or SIEM solutions.

3.4.4 Security functionality verification (SR 3.3 - IEC 62443-3-3)

3.4.4.1 The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

3.4.5 Input validation (SR 3.5 - IEC 62443-3-3)

3.4.5.1 The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.

3.4.6 Deterministic output (SR 3.6 - IEC 62443-3-3)

3.4.6.1 The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.

3.5 FR 4 – Data Confidentiality

3.5.1 Information confidentiality (SR 4.1 - IEC 62443-3-3)

3.5.1.1 The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

3.5.2 Use of cryptography (SR 4.3 - IEC 62443-3-3)

3.5.2.1 If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.

3.6 FR 5 – Restricted data flow

3.6.1 Network segmentation (SR 5.1 - IEC 62443-3-3)

3.6.1.1 The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

3.6.2 Independence from non-control system networks (SR 5.1 RE 2 - IEC 62443-3-3)

3.6.2.1 The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

3.6.3 Zone boundary protection (SR 5.2 - IEC 62443-3-3)

3.6.3.1 The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

3.6.4 General purpose person-to-person communication restrictions (SR 5.3 - IEC 62443-3-3)

3.6.4.1 The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.

3.6.5 Application partitioning (SR 5.4 - IEC 62443-3-3)

3.6.5.1 The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.

3.7 FR 6 – Timely response to Events

3.7.1 Audit log accessibility (SR 6.1 - IEC 62443-3-3)

3.7.1.1 The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

3.7.2 Continuous monitoring (SR 6.2 - IEC 62443-3-3)

3.7.2.1 The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

NOTE Response time is a local matter outside the scope of this standard.

3.8 FR 7 – Resource availability

3.8.1 Denial of service protection (SR 7.1 - IEC 62443-3-3)

3.8.1.1 The control system shall provide the capability to operate in a degraded mode during a DoS event.

3.8.2 Resource management (SR 7.2 - IEC 62443-3-3)

3.8.2.1 The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

3.8.3 Control system backup (SR 7.3 - IEC 62443-3-3)

3.8.3.1 The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.

3.8.4 Backup verification (SR 7.3 RE 1 - IEC 62443-3-3)

3.8.4.1 The control system shall provide the capability to verify the reliability of backup mechanisms.

3.8.5 Control system recovery and reconstitution (SR 7.4 - IEC 62443-3-3)

3.8.5.1 The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

3.8.6 Emergency power (SR 7.5 - IEC 62443-3-3)

3.8.6.1 The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.

3.8.7 Network and security configuration settings (SR 7.6 - IEC 62443-3-3)

3.8.7.1 The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.

3.8.8 Least functionality (SR 7.7 - IEC 62443-3-3)

3.8.8.1 The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.