This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Operational Technology/Industrial Control Systems (OT/ICS) Security Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Reasons for modification
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the modification >

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements to the Operational Technology/Industrial Control System (OT/ICS) for <organization name>. OT/ICS systems include all assets, devices and systems associated with Operational Technology (OT) infrastructure.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018, CSCC-1:2019 and OTCC-1:2022, in addition to other related cybersecurity legal and regulatory requirements.

Scope

The standard covers all systems residing in the OT/ICS network in the <organization name> and applies to all associated with OT/ICS personnel (employees and contractors) in the <organization name>.

Standards

1	General requirements
Objective	Define general requirements for OT/ICS systems to ensure that their availability, integrity and confidentiality are protected and they are securely managed and used appropriately when required.
Risk Implication	If OT/ICS systems are not used properly and its management process is not conducted in line with this security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.
Requirements	
1-1	All OT/ICS systems in <organization name> infrastructure must be deployed in line with approved cybersecurity policies,

	standards and requirements in order to ensure safety, security and proper functioning of the devices.
1-2	All OT/ICS systems must be identified, inventoried, managed, maintained and protected according to predefined standards, vendor guidelines, best practices and as per related laws and regulations.
1-3	OT/ICS systems must include all assets/systems responsible for performing and maintenance of <organization name>'s operations, including OT/ICS controllers like Programmable Logic Controllers (PLC's), Remote Terminal Units (RTUs), Distributed Controls Systems (DCS), Safety Instrumented Systems (SIS) and other assets responsible for controlling the <organization name>'s operations.
1-4	All OT/ICS systems must be managed during the entire system lifecycle in accordance with the "security-by-design" approach.
1-5	All documents required by the OT/ICS Security Standard must be in line with this standard and OTCC controls.
1-6	If it is possible, cryptographic hashes or checksums must be used to check OT/ICS controller code integrity and raise an alarm in case of change.
1-7	Process control system engineers must ensure that operators can only input or set what is practical or physically feasible in the process.
2	Access control
Objective	Define requirements for OT/ICS systems access configuration process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems' access is not defined and monitored, and its management process is not performed in line with <organization name>'s security standards, this can implicate

	access violations that could breach the business and operation continuity and cause financial losses.
Requirements	
2-1	<organization name>'s OT/ICS system resources must be used only by authorized users, programs, processes, or other systems.
2-2	Access to the OT/ICS systems must be granted only after user identification and authorization. <organization name> must define and document system account types and privileges.
2-3	Default accounts and passwords shall be deactivated or removed.
2-4	<organization name> must ensure mechanisms or procedures to protect systems in accordance with the <organization name>'s Access Management standards and general security practices based on the ISA/IEC 62443 or NIST SP 800-82r2 standards.
2-5	<organization name> must ensure that the access enforcement process for logical/physical access to OT/ICS systems does not impact or disturb the operational continuity.
2-6	Users must only be granted the rights which are strictly required for realizing their tasks (principle of least privilege). It should be particularly avoided to grant system administrator rights where possible. Accounts which are not required should be deactivated or removed if possible.
2-7	<organization name> must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
2-8	All remote sessions to OT/ICS systems must be secured, encrypted, and established in an accepted way which doesn't

	interfere or impact the OT/ICS operation. All remote connections and activities must be continuously monitored and recorded.
2-9	Public and unsecured access to OT/ICS systems must not be permitted. Access to OT/ICS systems from external networks must be allowed only through the dedicated DMZ area.
2-10	<organization name> must provide dedicated jump stations/hosts placed in DMZ to ensure strictly controlled access for external connections to OT/ICS systems.
2-11	OT/ICS controllers configuration, program and/or runtime data areas must be segregated based on the access medium, such as the physical interface, communication protocol and command type (levels of None, Read or Read/Write for the Configuration/Program and for the External Network).
2-12	Configuration or maintenance of OT/ICS controllers' access must be restricted to an authorized system administrator only and protected by non-default account and password.
3	Audit and accountability
Objective	Define requirements for the OT/ICS systems audit and accountability processes to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems audit and accountability are not defined and managed properly in line with <organization name>'s security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.
Requirements	
3-1	Audits of the security of OT/ICS networks and other components must be carried out at regular intervals. In

	complex systems, specialized teams must be established for the identification and assessment of possible attack scenarios.
3-2	Periodic audits of the OT/ICS must be performed to validate: ● The security controls present during system validation testing are still installed and operating correctly in the production system. ● The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur. ● The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.
3-3	In certain circumstances, where the OT/ICS systems cannot support the use of automated mechanisms to generate audit records, <organization name> must employ non-automated mechanisms or procedures as compensating controls in accordance with the general security practices based on the ISA/IEC 62443 or NIST SP 800-82r2 standards.
4	Assessment and monitoring
Objective	Define requirements for the OT/ICS systems assessment and monitoring processes to ensure proper and secure process flow according to defined security rules.
Risk Implication	Lack of OT/ICS systems assessment and monitoring can have severe implications regarding security. Lack of monitoring could result that unauthorized changes cannot be detected which could compromise the process and operation continuity.
Requirements	
4-1	Assessment processes must be performed by qualified OT/ICS assessors authorized by <organization name>.

4-2	Before implementing any security controls to OT/ICS systems, a proper risk assessment must be performed to ensure that implementation will not affect operations, or business continuity, and will not decrease security capabilities of the systems.
4-3	When conducting the risk assessment, <organization name> must assess whether the implementation of any security controls on OT/ICS systems will not affect other system components.
4-4	The assessors responsible for the assessment must fully understand the organizational (especially OT/ICS) security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process.
4-5	If an OT/ICS asset must be taken off-line to conduct an assessment (e.g. penetration tests, vulnerability scans), the assessment and/or scans must be scheduled to perform during planned OT/ICS outages whenever possible.
4-6	Vulnerability scanning and penetration testing must be used with care on OT/ICS networks to ensure that OT/ICS functions are not adversely impacted by the scanning process.
4-7	Vulnerability scans from the IT network must be blocked at network traffic level to ensure that they do not scan the OT/ICS network.
5	Backup management
Objective	Define requirements for the OT/ICS systems backup management process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems' backup management process is not defined and the backup process is not performed, this can

	have severe implications that could impact operation continuity and cause financial losses.
Requirements	
5-1	<organization name> must perform OT/ICS systems backups on a regular basis based on an OT/ICS dedicated procedure. The backup process must not affect operations, or business continuity.
5-2	Backups must cover all OT/ICS equipment dedicated to process control and monitoring (and must not be limited to Windows- and Linux-based machines only).
5-3	OT/ICS systems' backups process must embrace systems, programs, installed licences, components settings, and current and initial values of process variables.
5-4	OT/ICS systems' backups must be regularly updated and checked in a dedicated environment to not affect operations, or business continuity.
5-5	If backup is not possible to perform on running systems, it must be carried out during maintenance windows and must be planned in advance.
5-6	<organization name> must ensure backup retention rules. Backups must be prepared at least to cover state after SAT (Site Acceptance Test), and before all scheduled maintenance windows of OT/ICS systems.
5-7	All OT/ICS systems backups processes must be predefined, configured and automated (if possible).
5-8	<organization name> must provide a dedicated OT/ICS backup server.
5-9	OT/ICS backup server network must be isolated physically or logically from the rest of the OT/ICS network.

6	Configuration management
Objective	Define requirements for the OT/ICS systems configuration management process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems' baseline configurations are not defined and the configuration management process is not performed in line with <organization name>'s security standards, this can have severe implications that could breach the process and operation continuity and cause financial losses.
Requirements	
6-1	Configuration for all authorized OT/ICS systems in <organization name> must be documented and must be maintained and followed by all respective asset owners.
6-2	Configuration management policy and procedures must be developed and used to control modifications to hardware, firmware, software, and documentation to ensure that the OT/ICS system is protected against improper modifications prior to, during, and after system implementation.
6-3	Baseline security configurations for OT/ICS systems including connectivity, operational, and communications aspects of systems must be developed, documented and formally reviewed.
6-4	OT/ICS systems in a critical environment must be configured in such a way that they provide as few points of attack as possible and only support the required functions. All unused functionalities, services, protocols and ports must be disabled.
6-5	Define and implement mechanisms to prevent currently running processes from being manipulated. Mechanisms shall be adjusted and tailored to the associated process.

6-6	OT/ICS systems' configuration shall be prepared and maintained following the least functionality principle. System configuration changes shall be embraced by the dedicated change management system.
6-7	Hardware interfaces should be deactivated or protected against access and misuse unless they are required for operational continuity.
6-8	All OT/ICS systems must use only fully supported and up-to-date operating systems.
6-9	All configuration changes must be logged and monitored. Log solution must be configured to send only specific logs to the central log system using syslog protocol and CEF, LEEF or RFC 5425 specified log format.
6-10	<organization name> must perform regular OT/ICS systems hardening to treat risks and vulnerabilities on systems. OT/ICS systems hardening includes (but is not limited to): ● patching operating systems and application software, ● upgrading of firmware, ● secure configuration, ● user and account access limitation, ● removal of unnecessary software and components.
6-11	<organization name> must continuously identify and analyze risks associated with legacy OT/ICS devices and systems operating within <organization name>'s network environment. For all legacy devices and those that cannot be patched, <organization name> must implement compensating controls e.g.: ● isolation of the devices, ● moving them into secured network segments,

	● limit communication only to the necessary services, ● implement sandbox devices/systems which will pretend original ones, ● introducing micro-segmentation.
6-12	If OT/ICS controllers offer the ability to deactivate physical ports, network services and individual commands, all unused features must be deactivated.
6-13	Easily exploitable features such as embedded webserver or less commonly used features must be disabled.
6-14	All OT/ICS controllers' real time clocks must be synchronized using relevant mechanisms like Network Time Protocol (NTP) or Precision Time Protocol (PTP).
6-15	OT/ICS controllers must be protected from manipulation of mode switches, IP address changes, or controller node number identifier changes.
6-16	OT/ICS controller code must be splitted into modules, using different function blocks.
6-17	Operational logic must be left directly in the OT/ICS controllers, not in HMIs or other machine interfaces.
7	Continuity planning
Objective	Define requirements for the OT/ICS systems continuity management process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems continuity planning is not defined and managed properly and its management process is not conducted in line with <organization name>'s security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.

Requirements	
7-1	<organization name> must define OT/ICS continuity plans and disaster recovery procedures for categories of disruptions or failures in accordance with the <organization name>'s Cybersecurity Business Continuity Policy and general business continuity practices based on the ISA/IEC 62443 or NIST SP 800-82r2 standards.
7-2	In the event of a loss of processing within the OT/ICS or loss of communication with operational facilities, the OT/ICS systems must execute predefined procedures (including system state variables restoration).
7-3	In situations where <organization name> cannot test or exercise the continuity plan or disaster recovery plan on OT/ICS production due to significant adverse impact on performance, safety, or reliability, <organization name> must employ appropriate compensating controls in accordance with the <organization name>'s Cybersecurity Business Continuity Policy, Backup and recovery management policy and standard, and general security practices based on the ISA/IEC 62443 or NIST SP 800-82r2 standards.
8	Incident response
Objective	Define requirements for the OT/ICS incident response plan to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS incident response plan is not defined and managed properly and its management process is not conducted in line with <organization name>'s security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.
Requirements	

8-1	<organization name> must define an OT/ICS incident response plan which defines procedures to be followed during intrusion to minimize the effect of its. Defined OT/ICS incident response plans must be integrated and aligned with organizational plans and its procedures such as IT incident response plans, crisis management, and Business Continuity Plan (BCP).
8-2	<organization name> must develop the dedicated playbook for incidents associated with OT/ICS systems.
8-3	All plans and playbooks must be developed in a way to prevent impact or disturb the operational, process and business continuity.
9	Maintenance
Objective	Define requirements for the OT/ICS maintenance to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS maintenance is not defined and managed properly and its management process is not conducted in line with <organization name>'s security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.
Requirements	
9-1	<organization name> must provide policy and procedure for performing routine and preventative maintenance on the OT/ICS components.
9-2	<organization name> must schedule in advance maintenance windows for all OT/ICS systems to not affect operations, or business continuity.
9-3	Maintenance rules and Service Level Agreement (SLA) must be defined and agreed with respective vendors of the OT/ICS

	systems to outline specific responsibilities and satisfy <organization name>'s expectations.
9-4	All OT/ICS systems must be supported and maintained during their entire lifecycle.
9-5	Out-of-date OT/ICS systems must be immediately updated during dedicated OT/ICS outages.
9-6	Unsupported OT/ICS systems must be immediately upgraded/migrated or in particular cases covered by dedicated security controls.
10	Network security
Objective	Define requirements for the OT/ICS network security to ensure proper and secure process flow according to defined security rules.
Risk Implication	Lack of OT/ICS network protection can have severe implications that could breach the environment and process which can have an impact into operation continuity and cause financial losses.
Requirements	
10-1	Traffic between OT/ICS and IT networks must be restricted and there must be a single point of connection between these two networks and all traffic must go through the perimeter firewall.
10-2	<organization name> must implement reference network architecture based on the ISA/IEC 62443 standard and reference architecture model (Purdue model) differentiating at least following layers: ● IT network, ● IT/OT DMZ (demilitarised zone), ● OT/ICS supervisory network,

	● OT/ICS process network.
10-3	Every OT/ICS asset must be associated with a specific network layer.
10-4	Network traffic within the OT/ICS network and going through the IT/OT perimeter must be monitored, managed and controlled.
10-5	<organization name> must use and implement only dedicated OT/ICS network traffic monitoring tools. using passive monitoring methods and mechanisms.
10-6	OT/ICS intrusion detection systems used by <organization name> must be based only on passive traffic monitoring with developed attack signatures for various OT/ICS protocols and ensure that the use of them do not adversely impact the operational performance of the OT/ICS.
10-7	<organization name> must use next-generation firewalls as perimeter protection devices. Used firewalls must recognize and support industrial network protocols.
10-8	For critical systems where unidirectional network traffic is required, data diodes must be implemented according to the developed <organization name>'s Data diode standard.
10-9	<organization name> must establish configuration requirements, connection requirements, and implementation guidance for each type of OT/ICS wireless access. <organization name> must use only approved and secured OT/ICS wireless protocols in accordance with NIST SP 800-82r2.
11	Physical and environmental protection
Objective	Define requirements for the OT/ICS physical and environmental protection to ensure proper and secure process flow according to defined security rules.

Risk Implication	Lack of OT/ICS systems' physical and environmental protection can have severe implications that could breach the environment and process which can have an impact into operation continuity and cause financial losses.
Requirements	
11-1	The physical protection of the cyber components and data associated with the OT/ICS must be addressed as part of the overall security of a site.
11-2	<organization name> must provide physical security perimeters (several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or other informational systems). Physical security controls meant to protect physical locations include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures.
11-3	Access control systems must ensure that only authorized people have access to controlled spaces. A system must be able to verify that persons being granted access can be clearly and confidently identified. Access control should be highly reliable, yet not interfere with the routine or emergency duties of plant personnel (employees and contractors).
11-4	All environmental factors must be considered in addressing the security needs, e.g.: ● if a site is dusty, systems must be placed in a special, filtered cabinets, ● if vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems, ● systems and media must have stable temperature and humidity.

11-5	Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel (employees and contractors) during normal operation and emergency situations.
11-6	Reliable power for the OT/ICS systems is essential, so an uninterruptible power supply (UPS) or emergency generator must be provided. It must be sized, at a minimum, so that the system can be shutdown safely.
11-7	OT/ICS systems and other devices used for OT/ICS functions must never be allowed to leave the OT/ICS area and be used outside the OT/ICS network.
12	Risk assessment
Objective	Define requirements for the OT/ICS risk assessment to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS risk assessment procedures are not defined and managed properly and its management process is not conducted in line with <organization name>'s security standards, this can have severe implications that could breach the business and operation continuity and cause financial losses.
Requirements	
12-1	<organization name> must provide OT/ICS risk assessment policies and procedures to identify risks and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of an information system and data.
12-2	Estimation of potential risk of data flowing from the OT/ICS network to the corporate network impact must be defined on the basis of data business value.

12-3	OT/ICS risk assessment must embrace all factors that have impact on business continuity: cybersecurity, safety, physical security, operations continuity.
13	System, communication protection and information integrity
Objective	Define requirements for the OT/ICS system, communication protection and information integrity to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS system, communication protection and information integrity procedures are not defined and its management process is not conducted in line with <organization name>'s security standards, this can have severe implications that could compromise systems communication, which may breach operation continuity and cause financial losses.
Requirements	
13-1	<organization name> must select an appropriate failure mode for all OT/ICS systems.
13-2	On the application level, secure versions of protocols as well as accompanying mechanisms for encryption and the integrity and authenticity check must be used.
13-3	The use of cryptography must be determined after risk assessment and analysis of the security needs and the potential ramifications on system performance. <organization name> must consider whether latency induced from the use of cryptography would adversely impact the operational performance of the OT/ICS systems.
13-4	Before deploying encryption within an OT/ICS environment, solutions must go through extensive performance testing.

13-5	All cryptography solutions deployed and implemented for OT/ICS systems must be in accordance with developed Cryptography Policy and standards.
13-6	In certain circumstances, where the OT/ICS systems cannot protect the authenticity of communications sessions, <organization name> must employ compensating controls in accordance with the general security practices based on the ISA/IEC 62443 or NIST SP 800-82r2 standards.
13-7	Dedicated OT/ICS controls must exist for malicious code detection, spam and spyware protection, and intrusion detection.
13-8	The use of malicious code protection must be determined after careful consideration and after verification that it does not adversely impact the operational performance of the OT/ICS.
13-9	<organization name> must use Endpoint Protection System recommended by OT/ICS vendor: ● Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general purpose SCADA and backup servers must be secured in line with regular security practices based on the <organization name>'s Workstations Security standard, ● all other servers and workstations in the control systems environment (DCS, PLC, instruments) that have time-dependent code, modified or extended the operating system must follow vendor recommendations.
13-10	<organization name> must ensure that the use of monitoring tools and techniques does not adversely impact the operational performance of the OT/ICS.

13-11	OT/ICS systems must not be automatically shut down or restarted without system administrator permission upon the identification of an anomaly.
13-12	OT/ICS systems that are classified as critical to the <organization name> must be supported by redundancy and emergency shutdown systems to protect and ensure high process availability.
13-13	<organization name> must ensure that the use of integrity verification applications does not adversely impact the operational performance of the OT/ICS.
13-14	OT/ICS controllers must be monitored in terms of the frequency of abnormal activities and appropriate actions must be taken in case of detection.
13-15	Industrial communication protocols used by OT/ICS controllers must be known and well documented.
13-16	Communication protocols used by OT/ICS controllers to exchange data with the external from OT/ICS area point of view systems (solutions outside the OT/ICS area) must be recognizable by industrial firewall and dedicated IPS/IDS industrial tools.
13-17	Safe states for the process in case of OT/ICS controller restarts (e.g., energize contacts, deenergize, keep previous state) must be defined.
13-18	OT/ICS controllers’ diagnostics logs must be kept for potential analysis. Diagnostic logs must be sent to external log collector servers.
13-19	OT/ICS controllers hard stop events from faults or shutdowns must be logged and monitored to consult before controller restarts.

13-20	A memory usage for every OT/ICS controller deployed in the production environment must be measured and its trend identified for diagnostics. There must be a baseline provided for memory usage.
14	Vendor and third-party security management
Objective	Define requirements for the OT/ICS systems vendors and third-party to ensure proper and secure process flow according to defined security rules.
Risk Implication	If OT/ICS systems vendors do not ensure proper security resources in line with <organization name>'s security standards, this can have severe implications that could breach the process and operation continuity, compromise the organization and cause financial losses.
Requirements	
14-1	OT/ICS systems vendors must ensure regularly updated security advisory regarding used OT/ICS components.
14-2	OT/ICS systems vendors must ensure current and regularly updated vulnerabilities registers providing all detected vulnerabilities and potential ways to patch.
14-3	All OT/ICS systems vendors and third party contractors must be regularly monitored and assessed regarding the associated risk level (including Supply Chain risk) and agreed SLA.
14-4	All new OT/ICS systems vendors and third party contractors must be assessed in terms of possible risks and SLA.
15	Compliance
Objective	Define requirements for the OT/ICS systems compliance to ensure proper and secure process flow according to defined security rules and norms.

Risk Implication	Lack of OT/ICS systems compliance can have severe implications that could compromise the organization and cause financial losses.
Requirements	
15-1	All OT/ICS systems, its integrators and vendors must ensure compliance with OTCC controls and other dedicated industrial standards and norms like ISA/IEC 62443, NIST SP 800-82, and other specific requirements.
15-2	<organization name> must conduct regular compliance assessment.
15-3	All agreements with OT/ICS systems vendors and third party contractors must be regularly reviewed in terms of regulatory requirements and compliance.
16	Other Standards
Objective	The OT/ICS systems must be securely configured, monitored and performed appropriately when required.
Risk Implication	If <organization name> is not compliant with all of <organization name>'s standards and requirements, it could be exposed to severe threat rise.
Requirements	
16-1	The following standards must be implemented in relevance to OT/ICS systems security: 1. Network Security Standard 2. Workstation Security Standard 3. Identity and Access Management Standard 4. Secure Configuration and Hardening Standard 5. Backup and Recovery Management Standard

	6. Physical Security Standard 7. Assets Management Standard 8. Asset Classification Standard 9. Cybersecurity Event Logs and Monitoring Management Standard 10. Incident Response Standard

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <OT/ICS security function>

4- **Standard Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.