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.

Data Diode 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	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

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 related to the data diodes for <organization name> in order to minimize cybersecurity risks resulting from internal and external threats. Data diodes is a network appliance or device allowing data to transmit only in one predefined direction

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

The standard covers all data diodes installed in the <organization name>'s OT network and applies to all personnel (employees and contractors) in the <organization name>.

Standards

1	General Requirements
Objective	Define general requirements for data diodes to ensure that its availability, confidentiality and integrity are protected, and they are securely managed, and used appropriately when required.
Risk Implication	If data diodes are not used properly or misconfigured and its management process is not conducted in line with general security standards, this can have severe implications that have a breach and disrupt the business and cause safety incidents or financial losses.
Requirements	
1-1	All data diodes in <organization name> architecture must be deployed in line with developed cybersecurity policies, requirements and as per related laws and regulations.

1-2	All data diodes must be identified, inventoried, managed and protected in line with the defined ICS assets cybersecurity standard.
1-3	The data diode must be compliant with best practice Industrial Cybersecurity standards (e.g. IEC 62443, NIST SP 800-82).
1-4	The data diode must only allow data flow from one network to another with physical and logical isolation.
2	Access Control
Objective	Define requirements for the data diode access configuration process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If data diode access is not defined and managed properly and its management process is not conducted in line with security standards, this can have severe implications that could breach the business and operating continuity and cause financial losses.
Requirements	
2-1	The data diode must have a dedicated and separated network management interface.
2-2	The data diode must have a dedicated Graphical User Interface (GUI) or Command Line Interface (CLI) dedicated to performing device configuration.
2-3	Data diode configuration or maintenance shall be restricted to authorised system administrators only.
2-4	Access to the data diode configuration shall be protected by non-default accounts and passwords.

2-5	Physical access to the data diode must be restricted to authorised system administrators only and protected by physical security perimeters.
3	Configuration Management
Objective	Define requirements for the data diode configuration management process to ensure proper and secure process flow according to defined security rules.
Risk Implication	If data diode basic configurations are not defined and the configuration management process is not performed in line with security standards, this can have severe implications that could breach the process and operating continuity and cause financial losses.
Requirements	
3-1	Baseline security configurations for data diodes including connectivity, operational, and communications aspects of systems must be developed, documented and formally reviewed.
3-2	The management/diagnostic interface must provide a possibility to log events and forward them to other security systems or log servers.
3-3	The data diode must provide backup and restore functions to allow administrators to export and import data diode settings.
3-4	The data diode must collect and forward logs of any events that may be defined in the scope of audit inspection.
3-5	The data diode solution must be configured to send only specific logs to the central log system using e.g. SYSLOG protocol and CEF, LEEF or RFC 5425 specified log formats.

4	Physical and Environmental Protection
Objective	Define requirements for the data diode physical and environmental protection to ensure proper and secure process flow according to defined security rules.
Risk Implication	Lack of data diodes physical and environmental protection can have severe implications that could breach the environment and process which can have an impact into operating continuity and cause safety incidents or financial losses.
Requirements	
4-1	If necessary, the data diode must be made in a ruggedized version designed to operate reliably in harsh usage environments and conditions, such as strong vibrations, extreme temperatures and wet or dusty conditions.
4-2	The data diode must be adapted to be mounted in an industrial environment (rack cabinet or DIN rail).
4-3	The data diode hardware components must ensure high availability (e.g. redundant power).
5	System and Communication Protection
Objective	Define requirements for the data diode system and communication protection to ensure proper and secure process flow according to defined security rules.
Risk Implication	If the data diode system and communication protection procedures are not defined and its management process is not conducted in line with security standards, this can have severe implications that could compromise systems communication, which may breach operating continuity and cause safety incidents or financial losses.
Requirements	

5-1	The data diode must be installed above the DMZ from the OT side on DMZ/IT perimeter as a single point of connection between industrial, protected source zone and other untrusted networks/zones.
5-2	The data diode must only accept data from known whitelisted data sources that could be restricted to a unique combination of IP addresses, network ports and/or protocols.
5-3	The data diode transfer throughput must be set up to a specific value (in Mbits/s), which needs to be defined based on the transfer throughput estimation and simulation testing.
5-4	The data diode must support industrial protocols used to exchange data between the industrial, protected source zone and DMZ, business, untrusted destination networks/zones used by <organization name>.
5-5	The data diode shall support and recognize open automation protocols and historians protocols (i.e. MODBUS, OPC UA, etc.).
5-6	The data diode shall support and recognize additional network protocols used for operation support or file transfer, (e.g. TCP, FTP, SFTP, CIFS or NTP).
6	Other Standards
Objective	Data diodes must be securely configured, used and monitored.
Risk Implication	If <organization name> is not compliant with all of standards and requirements, it could be exposed to increasing threats which may breach operating continuity and cause safety incidents or financial losses.
Requirements	

6-1	The following standards must be implemented in relevance to ICS assets security: 1. OT/ICS Security 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 employees 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.