Document number	TPL TECH MC&I STD PCE Security Controls Framework-006
Business Name	Transnet Pipelines
Process/ Activity Name	Framework for Minimum Controls for Security in the Process Control Environment
Process Owner Name	Mabjana Percy Matenchi
Process Owner Signature	
Version Number	3.0
Classification	Unclassified
Effective Date	March 2024
Review Date	March 2029

SUMMARY VERSION CONTROL

VERSION NO.	NATURE OF AMENDMENT	PAGE NO.	DATE REVISED
1	Original Document	N/A	June 2007
2	Review		May 2013
3	Reference documents for risk management and align to NIST Cyber Security Framework	3	March 2024

Note: Only latest amendments and/or additions are reflected in italics in the body of the document

TABLE OF CONTENTS

1. Introduction

Process Control Systems (PCS) a subset of the Process Control Environment, although based on standard ICT technologies, have significantly different operational environments to that of the corporate ICT environment.

This framework utilises standard ICT security tools and techniques tailored to protect the Process Control Environment and its systems.

The framework will cover the principles and requirements for:

- Identification of the systems and equipment utilised by Transnet Pipelines in the Process Control Environment
- Protection and classification the risks associated with securing such equipment in a networked environment.
- Guidelines for implementation of secure architecture
- Ensuring Anomalies and Events are detected, and their potential impact is understood.
- Establishing response capabilities
- Recovery Planning processes and procedures to restore systems and/or assets affected by an incident.
- Awareness and skills
- Third party risk
- On-going governance

Security risks are classified on three levels:

- Low - classified as limited adverse effect on Organisational operations.
- Moderate - classified as serious adverse effect on Organisational operation.
- High - classified as catastrophic adverse effect on Organisational operations.

2. Business Risk

The Transnet Integrated Risk Management Policy document number TG/TGR12/1/1/1P and Transnet Enterprise Risk Management Methodology Strategy and Framework will be followed when conducting risk management for Process Control Environment. Risks will be identified, analysed, evaluated, mitigated, and reported using a risk register.

Security risks are classified on three levels as defined in the risk process**.**

2.1. Systems

Identifying and record physical and software assets within the Process Control System to establish the basis of an Asset Management. Document as minimum: station, system make and model, role of system, system name and software installed on the respective systems.

2.2. Threats

Protection and classification of the risks associated with securing such equipment in a networked environment.

2.3. Impacts

Identify potential impacts and consequences to the process control systems should a threat be realised. Loss of process control, loss of reputation, violation of regulatory requirements (health, safety and environment), inability to meet business commitments, financial loss, criticality in supply chain service and other key services. Ensure Anomalies and Events are detected, and their potential impact is understood.

2.4. Vulnerabilities

Evaluation of the infrastructure, operating system, applications, component software, network connections, remote access connectivity, processes, and procedures.

2.5. Undertake on-going assessment of business risk

Business risk is a function of threats, impacts, and vulnerabilities. Any changes to parameters or system modification could change the business risk. The change control process is used to identify any of these changes, initiating a re-evaluation of the business risk and appropriate security improvements.

3. Secure Architecture

Based on the identified risk, selection of technical, procedural and management protective measure to increase the security of the process control environment is implemented in accordance with best practice principles as detailed in API 1164 Pipeline SCADA Security as guidelines for Critical Infrastructure and the "Confidentiality, Integrity Availability" CIA triad model for data protection thus providing a secure operating environment.

CIA –

Confidentiality - only authorized user can access specific assets.

Integrity - data is correct, authentic, and reliable.

Availability - data is accessible to those that are authorized.

3.1. Network Architecture

- Identify all connections in the process control environment.
- Reduce the number of connections to the process control environment and ensure that there is a valid business case for the remaining connections.
- Segregate or isolate process control systems from other networks
- Implement dedicated infrastructure for mission or safety critical process control systems.
- Remove, where possible, TCP/IP connections between safety systems (emergency shutdown systems) and process control systems or other networks. Where this is not possible, a risk analysis must be undertaken.

3.2. Firewalls

- Protect connections between the process control systems and other systems with a firewall and demilitarised zone (DMZ) architecture.
- Firewall configuration must be subject to review.
- Firewall changes to follow change control process.
- Implement appropriate firewall management and monitoring.

3.3 Remote Access

- Maintain an inventory of all remote access connection and types (virtual private networks or modems)
- Ensure that a valid business justification exists for all remote access connections
- Implement appropriate authentication mechanism for remote access connections
- Carry out regular audits to ensure that are no unauthorised remote access connections
- Implement appropriate procedures and assurance mechanisms for enabling and disabling remote access connections
- Restrict remote access to specific machines for specific users and if possible at specific times
- Ensure that remote access computer are appropriately secured (antivirus, anti-spam and personal firewalls)

3.4. Anti-virus

- Protect process control systems with anti-virus software on workstations and servers. Where anti-virus software cannot be deployed other protection measures must be implemented (gateway anti-virus scanning or manual media checking).
- Obtain accreditation and configuration guidance from process control system vendors prior to deployment of such software.

3.5. E-mail and internet access

- Disable all e-mail functionality from process control systems.
- Disable all internet access from process control systems unless defined in the architecture and within a DMZ.

3.6. System Hardening

- Undertake hardening of process control systems to prevent network based attacks. Remove or disable unused services and ports in the operating systems and applications to prevent unauthorised use.
- Ensure all inbuilt system security features are enabled.

3.7. Backups and Recovery

- Ensure effective backup and recovery procedures are in place, and are appropriate for the identified electronic and physical threats. These should be reviewed and regularly tested.
- Test the integrity of backups and document.
- Store backups at on and off site locations.

3.8. Security Controls - Physical security

- Deploy physical security protection measures to protect process control systems and associated networking equipment form physical attack and local unauthorised access. A combination of protection measures is to be considered which could include, drive locks, tamper proof casing, secure server rooms, access control systems and CCTV.

3.9. System Monitoring

- Monitor in real-time process control systems to identify unusual behaviour which might be the result of an electronic incident (increased amount of network activity etc.) Parameters are to be defined and monitored in real-time and compared with system baselines for normal operation to provide an indication of unusual behaviour.
- Utilisation of intrusion detection and prevention configuration to provide a more granular view of network activity.
- Review and analyse regularly a defined suite of process control system log files. Backup important log files and protect them from unauthorised access or modification.
- Log access to secure area.

3.10. Wireless Networking

- Deploy security protection measures to protect control systems and associated equipment from unauthorized access.

3.11. Security Patching

- Implement process for deployment of security patches to process control systems.
- Process to cater for vendor certification, testing of patches prior to deployment and a staged deployment process to minimise the risk of disruption due to change where possible.
- Where security patching is not possible or practical, alternative appropriate protection measures should be considered.

3.12. Passwords and Accounts

- Implement and enforce a password policy for all process control systems that cover strength of passwords and expiration times. Passwords are to be changed frequently, but where this is not possible or practical, alternative appropriate protection will be considered and documented.
- Regularly review all access rights and decommission old access accounts.
- Change vendor defaults passwords where possible.
- Passwords may not be deemed necessary for some functions e.g. view only.
- Stronger authentication methods for critical functions are to be considered.

3.13. Minimum security framework documentation

This documentation will be subjected to regular review and be updated to reflect current threats.

Documentation includes:

- Full inventory of the process control systems and components
- Known vulnerabilities as identified by the supporting reference documentation, API Standard 1164 and MC&I risk register.
- All process control system documentation will be secured, and access limited to authorised personnel.

3.14. Security Scanning

- Implement security scanning where possible for vulnerability management. Risks related to scanning process control systems should be considered before performing such scans and should only be considered during shut down conditions. Full risk assessments are to be carried out prior to any scanning activities.

3.15. Starters and leavers process

- Procedures will be followed to ensure that new starters receive the appropriate accounts, authorisation levels and training when they join the process control team.
- Procedures will be followed to ensure that confidential information and documentation is retrieved, accounts are deactivated and passwords are changed when personnel leave the process control teams or when team members change roles and responsibilities.

3.16. Management of Changes

- All systems will be subjected to the change control process. Security assessments will be included in these processes. Where necessary some changes may be required to be assessed and approved by multiple change control processes

3.17. Security Testing

- Security testing will be carried out where possible e.g. penetration testing. This testing must be conducted during shut downs or on backup systems where available

3.18. Device connection procedures

- Procedures will be followed to verify that devices are free from virus or worm infections before being connected as applicable.

4. Response Capabilities

A formal response management process will ensure that any changes to risks are identified as early as possible.

Routine assessments of the process control system security will be undertaken to identify, evaluate, protect and respond to new vulnerabilities, changes in security threats and electronic security incidents (e.g., worm or hacker attacks).

- The MCC Specialist and/or Administrator will respond to suspected security incidents.
- Appropriate electronic security response and business continuity plans are in operation for all process control systems.
- Electronic security plans are regularly maintained and tested.
- Processes and procedures to monitor, asses and initiate responses to security alerts and incidents (e.g., increase vigilance, isolate system, apply patches, initiate BCP).
- All process control security incidents are formally reported and reviewed.

5. Manage third party risk

The security of the process control environment can be subjected to significant risk by third parties such as vendors, support organisations and other links into the supply chain. Third parties will therefore be engaged and steps taken to reduce these potential risks.

5.1. Identify third parties

- Identify all third parties, including service providers and all their links into the supply chain that are associated with the process control environment.

5.2. Manage risk from vendors

- Security clauses will be detailed in all procurement contracts prior to agreements.
- Engage with all vendors on an ongoing basis to ensure that any current and future discoveries of vulnerabilities within the systems that they supply are identified and notified promptly to Transnet Pipelines.
- Request vendors to provide security guidance for their current control systems and a security roadmap for future system development.
- Ensure that all vendors incorporate appropriate anti-virus protection within their process control systems.
- Establish with the vendors an effective patching process.
- Agree with the vendor system hardening procedures for the process control systems in operation.
- Identify all component technologies (e.g. databases) used within the PCE to ensure that all vulnerabilities are managed.
- Undertake regular security reviews and audits of all vendors.

5.3. Manage risk from support organisations

- Undertake regular risk assessments of support organisations and ensure any required countermeasures are implemented.
- Prevent access to the PCE by support organisations until appropriate measures to prevent or reduce potential security breaches have been implemented. Issue and agree a contract defining the terms of the connection.
- Engage with all support organisations on an ongoing basis to ensure that any current and future discoveries of vulnerabilities within their systems that interact with the enterprise PCE are identified and notified to Transnet Pipelines.
- Increase awareness of all support organisations to fully understand the process control systems that they are supporting and agree to undertake such support in accordance with agreed security procedures.

5.4. Manage risk in the supply chain

- Engage with any organisation linked to the PCE through the supply chain to provide assurance that their process control security risks are managed.

6. Project interface

- Identify and engage all projects that impact on the PCE at an early
- stage of their development.
- Ensure that a security architect is appointed as a single point of accountability for the security risk management for the full life cycle of the project.
- Ensure standard security clauses and specifications are incorporated in all procurement contracts.
- Include security requirements in the design and specification of projects and ensure that all appropriate security policies and standards are adhered to.
- Undertake security reviews throughout the project development life cycle.
- Plan for security testing at key points of the project development life cycle (e.g. tender, FAT and commissioning).

7. On going governance

Formal governance for the management of the PCE security will ensure that a consistent and appropriate approach is followed throughout Transnet Pipelines.

7.1. Roles and responsibilities

- Impacts of legal and regulatory requirements on PCE security are to be regularly reviewed.
- PCE security practices are to be reviewed for alignment with the business and operational needs.
- Roles and responsibilities for all elements of PCE security are to be reviewed.
- Accountability for PCE security and management of associated risks resides with the MC&I Principal Engineer and responsibility is entrusted to the applicable MCC Specialist.

7.2. Policy and standards

- Formal policy and standards for PCE control system security reflecting Transnet Pipelines requirements and supporting business requirements has been developed and adopted and will be managed under change control.

7.3. Compliance with policy and standards

- An assurance programme will ensure that the PCE policy and standards are complied with on a continuous basis.

7.4. Updating Policy and Standards

- An on-going revision programme will ensure that the PCE security policy and standards are regularly reviewed and updated in-line with current threats and changes in legal and regulatory requirements and changes in the business and operational requirements.

8. References

- Transnet Pipelines Automation Standard
- API Pipelines SCADA Security Standard 1164
- National Institute of Standards and Technology - Cyber Security Framework for Critical Infrastructure (NIST CSF)
- MC&I Risk Register
- ISA/IEC 62443