Subject: IT Operations Security Policy

Business Unit: All

Function: IT

Territory: Global

Policy Number: E-IT-GL015

Effective Date: April 1, 2021

Policy Owner: VP of Information Security (J. Bociek)

1. PURPOSE

The purpose of this policy is to maintain Information Technology (IT) Operations security at Tenneco, safeguard the security and privacy of information and information assets and ensure Tenneco is compliant with applicable legislations and standards.

2. POLICY

IT Operations Management

2.1. IT Operations documentation may only be made available to Tenneco employees, contractor or approved third parties who have signed a Non-Disclosure Agreement (NDA), on an "as-needed basis".

2.2. Wherever possible, segregation of duties shall be implemented in all IT operational processes for reducing the risk of accidental or deliberate system misuse.

2.3. IT Operations shall:

- Document and maintain network diagram and network configuration.
- Implement and operate technology infrastructure and associated processes based on reference architecture and relevant policies.
- Maintain build and installation documentation for all authorized hardware.
- Maintain installation and configuration documentation for all authorized software
- Monitor security vulnerability for all Tenneco IT systems and devices.
- Non-production environments shall be separated from production environments to minimize the risks of unauthorized access or changes to the production system.
- Access to production data shall be governed by appropriate authorization.

2.4. Operations shall develop and maintain documentation describing IT operations processes, procedures and standards it follows in accordance with Tenneco policies and standards. This shall include, but is not limited to the:

Access Control:

- Tenneco shall implement access control measures that appropriately limit access to information, systems, and facilities to authorized individuals, based on legitimate business purposes.
- Tenneco shall establish, document, implement, and maintain Access Control standards, processes, and procedures to ensure only authorized individuals, who have a justified and approved business need, receive access to information systems based on least privilege principle.
- Components of Access Control shall include authentication, authorization, provisioning, termination, modification and recertification of all users.

Asset Management Procedures:

- All IT assets entrusted to IT Operations are deemed important as per the Asset Management Policy and shall follow the asset management guidelines outlined in the Asset Management Policy.
- Tenneco shall establish, document, implement, and maintain a systematic approach to identify information assets and define appropriate protection requirements.
- Tenneco shall document and maintain an inventory of assets associated with information and information systems throughout the entire lifecycle including acquisition, ownership, use, maintenance and disposal/removal.

Back-up and Recovery Procedures:

- Infrastructure and Operations shall develop, maintain and implement all procedures as defined in the Backup and Restore Policy.

Change Management Processes:

- All changes to Tenneco network systems shall follow a formal change management process and be reviewed and approved for execution by the appropriate parties, including Information Security.
- The change management process shall be fully documented according to the Information Technology Infrastructure Library (ITIL) Standard, outlining the steps and roles and responsibilities of all parties involved.

- The change management process shall be administrated by an independent group, separate from the teams requesting and/or implementing the changes.
- Tenneco shall ensure required system performance by consistently planning, configuring, maintaining and monitoring its information assets and processing facilities.

Compliance:

- Tenneco shall establish, document, implement, and maintain security Compliance standards, processes, and procedures to ensure compliance with regulatory and contractual requirements.
- Tenneco shall periodically review the operational and technical security controls for all Tenneco information assets based on regulatory, contractual and compliance requirement.

Disaster Recovery Plans and Procedures:

- IT Operations together with IT Security team shall develop, test and maintain disaster recovery plans and procedures.
- Tenneco shall ensure that its critical products, services, information, and information systems can be restored in a timely and secure manner following a significant disruptive event.
- Tenneco shall establish, document, implement, and maintain business continuity standards, processes, and procedures to ensure a minimum level of continuity for the delivery of critical products and services during a significant interruption. These shall include the process of development, testing, and maintenance of continuity plans for all critical processes and assets that support the delivery of the critical products and services.

Encryption Management:

- Tenneco shall implement cryptographic controls in compliance with Tenneco information classification and protection requirements in order to protect Tenneco's information assets.
- Tenneco shall establish, document, implement, and maintain encryption standards, processes, and procedures to ensure information assets containing restricted information are encrypted in accordance with applicable security standards as well as regulatory and contractual requirements. This includes the use of cryptographic controls as well as key management.

Information Assurance:

- Tenneco shall ensure that Tenneco information is protected throughout its lifecycle of creation, use, processing, storage, transmission and destruction, in accordance with the information's data classification.
- Tenneco shall establish and maintain an information classification and record classification scheme.
- Tenneco shall establish, document, implement, and maintain an information protection program that provides the requirements on the appropriate controls to protect Tenneco information, aligned with information classification.
- Information owners shall review the value and usefulness of information on a periodic basis. Owners also shall review the record/data retention schedule as issued by the Legal department to determine the minimum legal periods that information shall be retained.
- Tenneco shall destroy Tenneco information in accordance with the records management practices.

IT Risk Management:

- Tenneco shall implement a systematic approach to identify, assess, treat and monitor risks (including the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction) to information and information assets that support business processes and Tenneco's strategic initiatives.
- Tenneco shall establish, document, implement, and maintain IT Risk Management strategy, standards, processes, and procedures to ensure that emerging threats, and both internal and external risks that Tenneco is exposed to are identified, assessed, continuously monitored, and treated.

Logging and Monitoring Procedures:

Where applicable:

- IT Operations shall enable the audit logs in all IT systems recording user activities, exceptions, and information security events in accordance with the System Logging & Monitoring Policy.
- Logging facilities and log information shall be protected against tampering and unauthorized access.

- The audit log shall be reviewed on a regular basis as defined in the System Logging & Monitoring Policy.

Network Security:

- Tenneco shall ensure the protection of information in networks and its supporting information processing facilities. Tenneco shall control the flow of information between information assets in accordance with applicable security standards as well as regulatory and contractual requirements.
- Tenneco shall establish, document, implement, and maintain Network Security standards, processes, and procedures for networks processing Tenneco information to protect the network infrastructure, and information traversing the network or with external parties.

Patch Management Procedures:

- IT Operations shall develop, maintain and implement a patch management procedure to ensure patches to all Tenneco IT systems and applications are identified, tested and applied in a timely manner with minimal impact to the business process.
- Infrastructure and Operations shall provide IT Security, reports on the patch and updates implemented on a monthly basis or on demand.

Physical and Environmental Security:

IT Operations shall collaborate with the appropriate Tenneco teams to:

- Establish and document physical and environmental controls to prevent unauthorized physical access to Tenneco's IT information systems in order to protect them from damage, interruption, misuse, destruction and theft.

Security Incident Management:

- Tenneco shall define a consistent and effective approach for the management of information security incidents, including communication of security events and vulnerabilities.
- Tenneco shall establish, document, implement, and maintain Incident Response standards, processes, and procedures for reporting and responding to information security related events

on information assets, including Incident Identification, response, management, root cause analysis, and reporting.

Security Operations:

- Tenneco shall establish and maintain tools and processes to ensure controls are effective.
- Tenneco shall establish, document, implement and maintain secure operating standards, processes, and procedures.

Supplier Risk Management:

IT Operations shall collaborate with the appropriate Tenneco teams to:

- Ensure that supplier adhere to applicable security requirements, and that risks are continuously analyzed and managed.
- Establish, document, implement, and maintain supplier risk management standards, processes, and procedures inclusive of selection, contract review, risk assessment, monitoring, and management.

System Acquisition, Development and Implementation:

- Tenneco shall ensure that the acquisition, development or major modifications of technology follow secure development and implementation practices to help ensure the confidentially, integrity, and availability of information assets.
- Tenneco shall establish, document, implement, and maintain Information System Lifecycle Management standards, processes, and procedures to ensure secure operational management of all information assets throughout their lifecycles.
- IT Operations shall monitor and enhance the system’s performance, as well as make projections regarding future capacity requirements, to ensure the required system performance.
- IT Operations shall establish the acceptance criteria for supporting new information systems, upgrades and new versions. IT Operations shall also carry out appropriate tests of the system(s) during development and prior to acceptance.

System Hardening Procedures:

- IT Operations shall develop and maintain a system hardening procedure to ensure all new and updated IT systems are hardened to prevent security incidents.
- IT Operations shall develop and maintain system standard builds including build books and run books.

3. CONSEQUENCES

Failure to follow any Tenneco policy may result in disciplinary action, up to and including termination of employment.

4. REFERENCES

E-IT-GL007	Information Classification Policy
E-IT-GL004	Vulnerability Management Policy
E-IT-GL006	Disaster Recovery Policy