COMPUTER SECURITY

GENERAL PURPOSE

To provide a framework for the comprehensive governance of computer security for Marathon Petroleum Corporation "MPC") and its consolidated subsidiaries (the "MPC Group") and its Authorized Users in order to protect the company's computer systems, data, assets, infrastructure and computing environment and ensure its continued confidentiality, integrity and availability.

DEFINITIONS:

Authorized Users. Company employees and others performing services for MPC or its affiliates.

Computer Security. The protection and preservation of the company's Electronic Systems in order to ensure continued:

- Availability – Ensuring timely and reliable access to and use of the company's Electronic Systems
- Integrity – Safeguarding the accuracy and completeness of information and information processing methods within the company's Electronic Systems
- Confidentiality – Ensuring that the company's Electronic Systems are accessible only to those persons authorized to have access

Computing Domain. A collection of Electronic Systems and Authorized Users performing a common business function within the company. The company has identified two (2) Computing Domains:

1. Information Technology Computing Domain – The Computing Domain responsible for supporting corporate functions such as: management information systems, transaction processing systems, office support systems, and those systems where an Electronic System serves primarily as a decision support tool.

2. Operational Technology Computing Domain – The Computing Domain responsible for monitoring and controlling physical equipment and processes including, but not limited to: process control systems, SCADA systems, and those systems where an Electronic System primarily exercises a control function in its own right.

Defense-in-Depth. The implementation of multiple layers of security controls within a Computing Domain to provide Computer Security.

Electronic System. An interconnected system of electronic hardware, software, network connectivity, and data.

POLICY STATEMENT

Authorized Users

All Authorized Users share in the responsibility to protect the company's Electronic Systems to which they have access and will be held accountable for their Computer Security actions. Authorized Users' responsibilities include, but are not limited to:

- Reviewing, understanding, and complying with all company security policies, standards, and procedures
- Completing all required Computer Security training within designated timeframes
- Promptly reporting any known or suspected hardware, software, network, data or other Computer Security compromise to the company's Service Desk
- Safeguarding passwords and other sensitive access control information related to their own accounts or network access
- Not altering, tampering with, or destroying any Electronic System without authorization
- Not extending the physical network on which their system resides (e.g., installation of hubs, wireless access points, terminal services, etc.) without proper authorization
- Conducting themselves in a manner consistent with this Policy

Vice President and Information Security Officer

The MPC Vice President and Information Security Officer shall be responsible for all computer security activities related to the Computing Domains and has the authority to establish information security policies, standards, procedures and guidelines.

The MPC Vice President and Information Security Officer shall ensure that each Computing Domain:

- Develops and maintains a comprehensive governance process which includes Computer Security policies, standards, procedures, computer security risk management, Defense-in-Depth strategy, and compliance reviews
- Develops and presents training for Authorized Users within the Computing Domain
- Complies with all legislative and regulatory requirements

Policy Violations

Any Authorized User who violates this Policy or fails or refuses to cooperate with efforts to audit or otherwise implement this Policy may be subject to disciplinary action up to and including termination.

POLICY APPLICATION

This Policy applies to MPC and those entities within the MPC Group that have adopted it. Further, the substance of this Policy, appropriately adapted for the conditions involved, is recommended for adoption by MPC affiliate-operated joint venture entities.

POLICY ADMINISTRATION

The administration of this Policy is the responsibility of the MPC Senior Vice President, Chief Digital Officer.

POLICY REVIEW

This Policy shall be reviewed at least once every five years or when a significant change occurs, including any change in law, that impacts the content or substance of this Policy.

POLICY EXCEPTIONS

Modifications, waivers, limitations or exceptions of this Policy require the written approval of the MPC Senior Vice President, Chief Digital Officer.

REFERENCES

None