Policy: 6550-P9
Section: 6000 – Management Support

Procedure - Communications Security

Purpose
The purpose of this procedure is to ensure maintenance of the internal network security and to implement transfer procedures across all communication facilities for information assets that leave the organization.

External Segregation
Network Controls must segregate groups of information services, users and information systems when interconnecting networks to partners or other third parties.

A risk assessment must be performed to determine the necessary controls prior to allowing access of the ESD networks by new partners or third parties, and the Designated Information Security Officer (ISO) must approve of any such connections.

Network segregation controls will be selected on the basis of the risk assessment; cost and the impact of incorporating suitable routing and gateway technology. External connections must terminate in some form of controlled network (DMZ or similar) and must be subject to security controls. There shall be no direct connection between the ESD corporate (internal) network and any third party.

Internal Segregation
Based on site risk assessments, internal segregation of sites or networks within sites may be warranted. Development and testing networks/systems must be segregated from the rest of the internal network (either completely or through a firewall/proxy arrangement) to prevent malfunctions in software from impacting the rest of the network. In addition, certain locations (such as locations where there is civil unrest or rampant crime) must be adequately segregated from the rest of the network to ensure the security of corporate information assets.

Confidential information shall be consolidated and isolated on dedicated access servers, active storage and inactive storage (such as tape media) whenever possible.

Segregation of Development and Production Environments
ESD will separate development and production environments to prevent unfinished or malfunctioning software from affecting the business network. Only IT-approved systems will be connected to production environments, and only after the systems have fulfilled acceptance criteria.

Network Connection Control
Highly sensitive systems will have network access controls (i.e., firewalls or Access Control Lists) in place to prevent unauthorized connections from inside, or outside, ESD. This is in addition to any application or system access controls.

Network controls shall be configured to allow only network traffic required by the business to enter or leave the ESD network. The ISO shall work with management to determine those business requirements. These controls shall include:

- Ingress and egress filtering on border devices
- Firewall/access control list configuration that is host and port specific.

Risk assessments will be performed to establish which systems and/or applications should be protected.

Wireless Network Policy
All ESD-issued devices will connect to an internal wireless network that will be indicated appropriately.

All non-ESD issued devices, including personal devices, can connect to a guest wireless network that will be indicated appropriately.

Electronic Messaging
See Policy 2022 Electronic Resources and Internet Safety for general guidelines. Users of the ESD electronic communication systems will not send information assets deemed confidential, such as cardholder data, through any form of electronic messaging such as email, text, or chat.

Security of Physical Media in Transit
The organization will safeguard media or information commensurate with its data classification. All media in transit will be labeled accordingly and packed securely in accordance with the manufacturer's specifications. In consultation with IT, the system and/or data owner will approve the method for each transport of sensitive information.

Security of Electronic Media in Transit
The organization will safeguard media or information commensurate with its data classification. Sensitive information shall be protected from unauthorized access or modification. In consultation with IT, the system and/or data owner will approve the method for each transport of sensitive information.

Security of Electronic Media at Rest
The organization will safeguard media or information commensurate with its data classification. Sensitive information shall be protected from unauthorized access or modification. If using encryption, cryptography standards as defined in 2550-P6 Cryptography will be followed. In consultation with IT, the system and/or data owner will approve the storage of sensitive information.

Other Forms of Information Exchange
ESD staff shall work to protect the confidentiality and access to information that is communicated through other media such as voice, facsimile or video equipment.

Production of SPAM
ESD business units will take care not to produce Unsolicited Commercial E-mail (otherwise known as SPAM) to be sent out to the Internet. Any commercial e-mail should be specifically targeted to recipients in accordance with applicable laws and regulations.

Confidentiality

It is imperative that no ESD employees or agents disclose such information in any inappropriate ways, and that such information be used only in the performance of regular job duties.

Timeline for Implementation of Procedure

Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure’s periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.