UNITED STATES DISTRICT COURT
Middle District of Pennsylvania
IT Department

Security Awareness and Training Policy

Contents

Revision Log

Date	Description	Editor
Oct. 2019	Initial Policy	AL
April, 2020	Updated, signed and adopted	AL
Feb. 2021	No Update Required	AL
Feb. 2022	Changed Systems to IT	AL

Introduction

The United States District Court for the Middle District of Pennsylvania (PAMD) is committed to building and maintaining a Security Training and Awareness (SAT) Program that enables all end users to respond to Information Technology (IT) security issues that may occur while accessing Judiciary's Data Communication Network (DCN) and IT Department assets. Users are often called the first line of defense against IT security incidents. To successfully contribute to securing judiciary information, users must understand and follow good IT security practices. An effective IT Security Training and Awareness Program helps foster that understanding. Furthermore, employees should be provided with more detailed security training based on their roles and responsibilities. In this way, the Security Training and Awareness Program can empower each user to act securely.

Purpose

The purpose of this document is to establish and maintain an effective SAT model to further assist essential competencies of PAMD's user community realms of security training and awareness. Techniques and methods which are integral in facing the ever-changing security landscape.

Scope

This policy applies to all PAMD's employees, contractor personnel, interns/externs, and other non-government employees (collectively known as "end users") granted access to PAMD's information systems and excludes general access to PACER.

Roles and Responsibilities

The following roles and responsibilities are included in the PAMD SAT process:

Information Technology Security Officer (ISO) – The PAMD ISO is the SAT program manager for the court and is responsible for maintaining and executing the SAT plan, including the annual development of the SAT program activity matrix. The ISO identifies staff with security expertise to participate and contribute to the development of PAMD-specific security awareness content. The ISO identifies IT Department staff and other PAMD personnel who may benefit from additional specific role-based security training.

Information System Owners (SOs) - PAMD SOs provide insight into security-relevant issues specific to PAMD information systems.

Operations Manager – The Operations Manager is responsible for ensuring SAT Policy and Plan are documented, followed, and reviewed annually. The Operations Manager participates in more detailed SAT planning. The Operations Manager approves all role-based security training and security exercises for IT Systems Department staff having elevated system rights and privileges. The Operations Manager notifies the Human Resources (HR) Director of all role-based and external training completed by IT Department staff and any other court personnel.

Clerk of Court – The PAMD Clerk of Court has primary authority and responsibility for information security within the court and ensures that initial and annual security awareness refresher training is provided to PAMD personnel. The Clerk of Court reviews and approves the SAT Policy and Plan.

Human Resources Director – The PAMD HR Director, in compliance with the SAT Policy and Plan, ensures accurate records of both initial and refresher security awareness training are recorded and maintained. The HR Director receives and records notices of completion from the Operations Manager for all role-based or external IT security-related training completed by court personnel.

PAMD Help Desk – The Help Desk Service receives notification from HR and from IT regarding court workforce due for refresher security awareness training, role-based security training, or both. The Help Desk opens a ticket for each person and each training item. A notification is sent to each recipient with instructions for accessing training materials or attending a training session.

Court IT Department Staff – All PAMD IT personnel have elevated security rights and privileges in varying forms. Specific role-based security training is required at least quarterly for each IT Department staff member within their area of responsibility. IT Department staff may **not** act in their IT administrative capacity unless their related refresher training has been completed. The IT Department staff also develops and delivers general security awareness training and role-based security training.

General Court Staff – Prior to being granted system access, PAMD personnel will receive initial security awareness training as part of new personnel orientation and receive annual refresher training thereafter.

Interns, Externs, Temporary Staff, and Contractors – Prior to being granted system access, interns/externs, temporary staff, and contractors must receive initial security awareness training as part of new personnel orientation and receive annual refresher training thereafter.

Policy

In order to establish and maintain a robust Security Awareness and Training program, it is the policy of the PAMD:

- All court personnel for whom a user account is created must receive initial security awareness training within 30 days of beginning employment, although training prior to receiving system access is preferred.
- Security awareness refresher training must be provided annually in the month of October and completed by the end user within 30 days.
- Initial security awareness and annual refresher training must address court and national policies.
- Initial security awareness and annual refresher training should include best practices for both the use of and physical protection of judiciary information and IT systems.
- Additional security training must be provided:
    - To any personnel given specific IT role-based duties, based upon the level of sensitivity of IT activities,
    - When there is a change in status to any person assigned to handle information of a higher sensitivity,
    - To IT support personnel whenever new technologies or procedures are implemented (such as new firewalls, router technology, applications, etc.),
    - Whenever a new threat is identified (e.g., a threat such as spear phishing).
- Role-based security training must be completed prior to any exercise of IT administrative duties.
- Security awareness training records must be retained for a period of five years.
- The Security Training and Awareness Plan should be developed, implemented, and updated annually by the court IT Security Officer (ISO).

Guidance

Compliance Measurement

The IT Department and IT Security Officer will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the IT Director.

Exceptions

Any exception to the policy must be approved by the IT Director in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

Policy Review

The IT Security Officer, the Operations Manager, or designee will review this policy annually or upon events that warrant an earlier review.

References

Guide to Judiciary Policy, Volume 15, Chapter 3 § 340 IT Security Training and Awareness
http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#340

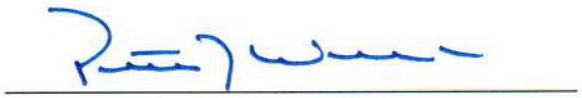
Guide to Implementing the Judiciary Information Security Framework

http://jnet.ao.dcn/information-technology/security/framework-shp/framework-guide

PAMD-Appropriate Use Security Policy

Policy Authorization

This IT Security Awareness and Training Policy was reviewed and approved by the Clerk of Court/CUE



Date: 3-2-20