FDIC DIRECTIVE 1360.16

Mandatory Cybersecurity and Privacy Awareness Training

Approval Authority: Sylvia Burns, Chief Information Officer and Chief Privacy Officer

Originating Division/Office: Chief Information Officer Organization

Approval Date: 04/05/2023

PURPOSE

This revised Directive provides policy and describe responsibilities for the mandatory Cybersecurity and Privacy Awareness Training (CPAT), which instructs authorized users on protecting information technology assets.

SCOPE

This Directive applies to all FDIC authorized users of FDIC information resources.

AUTHORITIES

See Appendix.

FORMS

None.

SUMMARY OF CHANGES

This Directive supersedes FDIC Circular 1360.16, Mandatory Information Security Awareness Training, dated July 23, 2002.

Under the programmatic authority provided by this updated Directive, FDIC Policy 09-008, Training Requirement for General Support System Administrators, is retired.

REVISION, dated April 5, 2023

This Directive had been revised to:

- Change the title from Mandatory Information Security Awareness Training to Mandatory Cybersecurity and Privacy Awareness Training;
- Align with the Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) requirements;
- Clarify Responsibilities; and
- Update definitions to remain consistent with National Institute of Standards and Technology (NIST), Computer Security Resource Center terms.

TABLE OF CONTENTS

PURPOSE 1
SCOPE 1
AUTHORITIES 1
FORMS 1
SUMMARY OF CHANGES 1
BACKGROUND 4
POLICY 5
A. Types of Training 5
B. Compliance 5
C. Disciplinary Action 6
RESPONSIBILITIES 7
A. Chief Information Security Officer, Office of the Chief Information Security Officer 7
B. Privacy Program Section, Office of the Chief Information Security Officer 7
C. Supervisors/Managers 7
D. System Owner or Project Owner 7
E. Information Security Managers 8
F. Authorized Users 8
G. Contracting Officers and Oversight Managers 8
APPENDIX 9
GLOSSARY OF TERMS 10
GLOSSARY OF ACRONYMS 11

BACKGROUND

The Federal Information Security Modernization Act of 2014, as amended (Public Law 113-283), requires each agency to develop, document, and implement an agency-wide information security program that includes awareness training.

OMB Circular A-130, Managing Information as a Strategic Resource, establishes policy for the management of federal information resources and requires agencies to develop, maintain, and implement mandatory agency-wide information security and privacy awareness and training programs for all employees and contractors.

Additionally, the Privacy Act of 1974, as amended (Title 5, United States Code [U.S.C.], Section 552a), and implementing guidance require agencies to ensure personnel meet training obligations that address the protection of privacy with respect to the Privacy Act of 1974 and the handling and safeguarding of personally identifiable information (PII).

The FDIC provides mandatory Cybersecurity and Privacy Awareness Training (CPAT), which informs authorized users of information security risks associated with their activities and of their responsibilities to comply with FDIC policies and procedures designed to reduce these risks.

POLICY

It is FDIC policy to protect the integrity, confidentiality, and availability of information assets by providing cybersecurity and privacy awareness training to authorized users.

A. Types of Training

1. Cybersecurity and Privacy Awareness Training

   The objectives of CPAT are to enhance awareness of the threats to FDIC information and information systems, provide methods to protect sensitive and personally identifiable information, and to encourage the use of sound information security practices within the FDIC. Authorized users:

   a. Complete CPAT within five business days of receiving FDIC equipment, and annually thereafter; and

   b. May extend the completion requirement for up to 21 days due to extenuating circumstances, with supervisory approval and concurrence from the Information Security Manager (ISM).[1]

2. Privileged User and Role Based Training

   The objectives of Privileged User and Role Based Training are to provide authorized users with significant security responsibilities, the understanding of risk management and various information security topics. Authorized users:

   a. Complete training prior to gaining privileged access to the FDIC's network and systems;

   b. Review and agree with the roles and responsibilities for the system(s) to which they are granted elevated access or permissions; and

   c. Complete required training courses on an annual basis to maintain access.

B. Compliance

1. Completion of Cybersecurity and Privacy Awareness, Privileged User, and Role Based Training is monitored by the Office of the Chief Information Security Officer (OCISO).

2. Upon completion of training and associated acknowledgement, the name, network identification, and agreement date are recorded in the FDIC's learning management system.

[1] The Division/Office ISM transmits approved extensions to servicedesk@fdic.gov.

3. Failure to complete training in a timely manner or adhere to the requirements of this Directive may lead to revoked authorized user access.

C. Disciplinary Action

Any disregard or abuse of the provisions of this Directive may subject the authorized user to disciplinary action. Disciplinary action is administered in accordance with applicable laws, contractual agreements, and regulations; FDIC Directives 2410.06, Standards of Ethical Conduct for Employees, and 2750.01, Disciplinary and Adverse Actions; and applicable collective bargaining agreements.

RESPONSIBILITIES

A. Chief Information Security Officer, Office of the Chief Information Security Officer:

1. Establishes and maintains the CPAT program, which communicates responsibilities, sources of assistance, available tools, and other resources to authorized users;

2. Reviews and updates the CPAT program on a quarterly basis to ensure that information remains current and relevant;

3. Coordinates the monitoring of user completion of required training; and

4. Provides authorized users with Role Based and Privileged User Training, if required, to obtain and retain necessary access.

B. Privacy Program Section, Office of the Chief Information Security Officer:

1. Develops and oversees the privacy-related training and content for the CPAT program, as well as for Privileged User, Role-Based, and other applicable advanced or foundational FDIC privacy awareness and training programs;

2. Reviews Role Based and Privileged User training that is developed by system owners to align with privacy guidance;

3. Ensures that CPAT and any other privacy awareness training are consistent with applicable privacy laws, policies, and best practices; and

4. Helps establish Rules of Behavior for authorized users with access to PII and develop policies and procedures to hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks.

C. Supervisors/Managers:

Ensure their staff completes required trainings.

D. System Owner or Project Owner:

1. Develops Role Based and Privileged User Training specific to the information resource for which they are designated as owner;

2. Ensures, in collaboration with OCISO, authorized users receive appropriate security training and comply with Rules of Behavior; and

3. Ensure authorized users complete required Role Based training prior to authorizing access.

E. Information Security Managers:

1. Ensure Division/Office compliance with required training and Rules of Behavior for information resources; and

2. Participate in OCISO-sponsored security training and awareness activities, including conferences and periodic meetings.

F. Authorized Users:

1. Complete required CPAT, Role Based Training, and Privileged User Training (as applicable) as described in this Directive and acknowledge completion in the FDIC's learning management system;

2. Achieve and maintain awareness to the threats and vulnerabilities concerning FDIC information resources; and

3. Protect FDIC data, information, and systems.

G. Contracting Officers and Oversight Managers:

1. Ensure contractors complete required CPAT, Role Based Training, and Privileged User Training (as applicable) as described in this Directive and acknowledge completion in the FDIC's learning management system; and

2. Ensure contractors achieve and maintain awareness to the threats and vulnerabilities concerning FDIC information resources and protect FDIC data, information, and systems.

APPENDIX

External Authorities:

- Public Law 113-283, Federal Information Security Modernization Act of 2014, as amended
- Title 5, U.S.C., Section 552a, Privacy Act of 1974, as amended
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
- OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-16, Information Technology Security Training Requirements
- NIST Special Publication (SP) 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61, Computer Security Incident Handling Guide

Internal Authorities:

- FDIC Directive 1300.04, Information Technology Acceptable Use
- FDIC Directive 1360.01, Automated Information Systems (AIS) Security Program
- FDIC Directive 1360.09, Protecting Information
- FDIC Directive 1360.20, Privacy Program
- FDIC Directive 2600.01, Learning and Professional Development
- FDIC Directive 2750.01, Disciplinary and Adverse Actions

GLOSSARY OF TERMS

Authorized User: Employees, contractor personnel, and any other lawful individuals authorized to use FDIC information resources.

Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology (IT).

Information Security Risk: The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of FDIC information.

Personally Identifiable Information: Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Privileged User: An authorized user enabled to perform security-relevant functions that ordinary users are not authorized to perform.

Project Owner: The lead of a project team that provides decision support and guidance to the entire project team and directs project members responsible for the team's performance in new training development.

Role-Based: User roles typically reflecting the tasks needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Rules of Behavior: Guidelines established for General Support Systems or major applications that hold users accountable for their actions and responsibilities for information security through standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program.

System Owner: A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

GLOSSARY OF ACRONYMS

CPAT: Cybersecurity and Privacy Awareness Training

ISM: Information Security Manager

NIST: National Institute of Standards and Technology

OCISO: Office of the Chief Information Security Officer

OMB: Office of Management and Budget

PII: Personally Identifiable Information

SP: Special Publication