FDIC DIRECTIVE 1360.09

Protecting Information

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

Originating Division/Office: Chief Information Officer Organization

Approval Date: 07/03/2023 **Pedestrian Change Date**: 03/02/2024

PURPOSE

This revised Directive provides policy on the rules of behavior for protecting information created, collected, and maintained by the Corporation.

SCOPE

This Directive applies to all FDIC Divisions/Offices.

AUTHORITIES

See Appendix.

FORMS

None.

SUMMARY OF CHANGES

This Directive supersedes FDIC Circular 1360.9, Protecting Sensitive Information, dated October 27, 2015.

REVISION, dated July 3, 2023

This Directive had been revised to:

- Expand the scope beyond solely “sensitive information” and replaces it with a policy of protecting information commensurate with the risk associated with the inappropriate access, use, disclosure, or destruction of the information; and
- Streamline the Directive to decrease unnecessary complexity.

PEDESTRIAN CHANGE, dated March 2, 2024

This Directive has been revised to:

- Update language in the “Overview” section to include references to Federal Information Processing Standards (FIPS) 199 and FDIC Conceptual Data Model for information categorization; and

- Add the definition of “Sensitive Information” to the Glossary of Terms.

TABLE OF CONTENTS

BACKGROUND

The FDIC creates, collects, and maintains various types of information in a variety of formats from both the public and private sectors to execute its mission. The FDIC is obligated under the Federal Information Security Modernization Act of 2014 (FISMA) and government-wide policy issued by the Office of Management and Budget (OMB) to adequately secure and safeguard the information.

POLICY

It is FDIC policy to establish rules of behavior for the protection of information created, collected, and maintained by the Corporation.

A. Overview

The Corporation protects FDIC information commensurate with the level of risk to the FDIC and content of the information. FDIC information is categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems; potential impact levels; and the FDIC Conceptual Data Model.[1]

1. Information that identifies a particular entity or individual carries higher risk than information that does not.

2. Information that is collected, accessed, used, transferred, or stored as part of executing FDIC official business (referred to as "Production Data") must be processed in an authorized environment in accordance with the following:

    a. Test Systems that replicate Production Data must be authorized in accordance with the FIPS baseline impact level of the corresponding Production System(s); and

    b. Test Systems may not, under any circumstances, have direct access to Production Data sources.

B. Physical, Administrative, and Technical Controls

To minimize security and privacy risks, authorized users must use the following physical, administrative, and technical controls:

1. Collect and retain information only when it is necessary to satisfy an FDIC business requirement.
2. Label information in accordance with its sensitivity and FDIC Directive 1350.04, Document Labeling.
3. Protect information in accordance with its sensitivity by:

    a. Limiting access to individuals with a legitimate business need commensurate with the principle of least privilege;

    b. Following approved encryption guidance for information that is electronically transmitted (for more information on how to transmit information outside of the FDIC, see the Encryption Guidance webpage and Data Labeling standards on FDICnet);

[1] For more information, see the Conceptual Data Model (CDM) webpage on FDICnet.

c. Printing information, when necessary, in accordance with the following best practices:

   1) Retrieving printed documents that contain FDIC information from shared printers as soon as they are printed;

   2) Using printers located in secured rooms or FDIC-approved home printers, when available, in compliance with FDIC Directive 1300.04, Information Technology Acceptable Use; and

   3) Report any uncollected printed documents with FDIC information to a responsible individual (e.g., supervisor/manager) to disseminate or discard, as appropriate.

d. Sending information via fax in accordance with the following best practices:

   1) When faxing documents containing FDIC information, retrieve the original from the sending fax machine and alert the recipient to retrieve the copy from the receiving fax machine;

   2) When expecting a faxed document containing FDIC information, monitor the fax machine closely and retrieve the fax as soon as it arrives;

   3) When available, use fax machines located in secured rooms; and

   4) Report any uncollected faxed documents with FDIC information to a responsible individual (e.g., supervisor/manager) to disseminate or discard, as appropriate.

e. Using portable storage devices in accordance with best practices (see the Encryption Guidance webpage on FDICnet for more information);

f. Securing physical assets (e.g., portable storage devices, computing devices, and paper documents);

g. Shipping data-bearing devices and paper documents via approved carriers in accordance with best practices; and

h. Destroying information through approved methods in accordance with FDIC Directive 1210.01, Records and Information Management Program.

4. Use appropriate encryption solutions (see the Encryption Guidance webpage on FDICnet for more information), which include:

   a. Digital rights management for FDIC documents;

b. Secure email for email recipients outside the FDIC;

c. Encryption software; and

d. Secure transmission of large files through externally hosted services.

5. Do not transport or remove information from authorized locations without prior management approval in accordance with the following:

   a. Only use portable media under authorized procedures (see the Encryption Guidance webpage on FDICnet for more information); and

   b. Track the shipment of information via postal service providers under authorized procedures (see the Express Mail Job Aid webpage on FDICnet for minimum requirements for shipping paper or electronic materials).

6. Do not leave information unattended in workspaces or in public.

7. Store physical copies of information in locked drawers or file cabinets.

8. Store electronic information only on FDIC-authorized systems.

9. Use masked, obfuscated, or synthetic data for testing or training purposes, unless otherwise approved by the Authorizing Official.

10. Disclose inappropriate access, use, disclosure, or destruction of information in accordance with FDIC Directive 1360.12, Reporting Information Security Incidents.

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 Officer:

Ensures that appropriate technical, administrative, physical, and personnel controls are incorporated into existing and new systems and applications, including all significant system and software modifications.

B. Chief Information Security Officer:

1. Implements the FDIC Information Security Program (in accordance with FDIC Directive 1360.01, Automated Information Systems [AIS] Security Program) and the FDIC Privacy Program (in accordance with FDIC Directive 1360.20, Privacy Program) to ensure effective implementation of information security and privacy controls;

2. Advises Divisions/Offices and the Authorizing Official on information security and privacy risks associated with information; and

3. Ensures the dissemination of information security and privacy requirements.

C. Authorizing Official:

Approves use of data (not masked, obfuscated, or synthetic data) for testing or training purposes in accordance with the approved system security plan.

D. Division/Office Directors:

Enforce the protection of information commensurate with the level of risk.

E. Supervisors/Managers:

Assist their employees in identifying risk associated with FDIC information and ways to appropriately safeguard such information.

F. Employees:

Protect information in compliance with the policy outlined in this Directive.

G. Contracting Officers and Oversight Managers:

1. Ensure FDIC contract awards contain clauses requiring compliance with this Directive; and

2. Assist contractors in identifying risk associated with FDIC information and ways to appropriately safeguard such information.

APPENDIX

External Authorities:

- Public Law 100-235, Computer Security Act of 1987
- Public Law 113-283, Federal Information Security Modernization Act of 2014 (FISMA)
- Title 5, United States Code, Section 552a, Privacy Act of 1974, as amended
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61, Computer Security Incident Handling Guide
- OMB Circular A-130, Managing Information as a Strategic Resource

Internal Authorities:

- FDIC Directive 1300.04, Information Technology Acceptable Use
- FDIC Directive 1350.04, Document Labeling
- FDIC Directive 1360.01, Automated Information Systems (AIS) Security Program
- FDIC Directive 1360.12, Reporting Information Security Incidents
- FDIC Directive 1360.16, Mandatory Cybersecurity and Privacy Awareness Training
- FDIC Directive 1360.20, Privacy Program

GLOSSARY OF TERMS

Authorizing Official: A senior federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the United States.

Digital Rights Management: Technologies used by information holders to attempt to control how information is accessed and used.

Encryption Solutions: Technology used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading the data.

Federal Information Processing Standard: Standards and guidelines for federal computer systems that are developed by NIST in accordance with FISMA and approved by the Secretary of Commerce.

Information: Any communication or representation of knowledge, such as facts, data, or opinions in any medium or form (e.g., textual, numerical, graphic, cartographic, narrative, or audiovisual).

Masked Data: Test data that has systematically had a field removed or replaced with a value in a way that does not preserve the analytic utility of the value.

Obfuscated Data: Data that has been distorted by cryptographic or other means to hide information.

Physical, Administrative, and Technical Controls: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Principle of Least Privilege: The principle that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Privacy Controls: The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

Production Data: Information that is stored, processed, or transferred to execute FDIC business.

Production System: Any system that stores, processes, or transfers Production Data to execute FDIC business.

Sensitive Information: Any information, where the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of the FDIC in carrying out its mission or the privacy to which individuals are entitled. It includes, but not exclusively, the following:

1. Information that is exempt from disclosure under the Freedom of Information Act (FOIA), such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports;

2. Information under the control of the FDIC and contained in a Privacy Act system of record that is retrieved using an individual's name or by other criteria that identifies an individual;

3. Personally Identifiable Information (PII) about individuals maintained by the FDIC that, if released for unauthorized use, may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (e.g., Social Security Number) or a combination of two or more items (e.g., full name along with, financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud;

4. Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities; and

5. Information related to information technology specific to the FDIC that could be misused by malicious entities (e.g., internal IP addresses, server names, firewall rules, encryption and authentication mechanisms, and network architecture pertaining to the FDIC).

Synthetic Data: Data resulting from use of example production data to create artificial data that has some of the same statistical characteristics as an original data set.

Test System: Any system (e.g., Quality Assurance, Development, and Laboratory environments) that is used to develop, modify, or evaluate changes to Production Systems and may support multiple Production Systems. A Production System may also be supported by multiple Test Systems.

GLOSSARY OF ACRONYMS

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Modernization Act of 2014

NIST: National Institute of Standards and Technology

OMB: Office of Management and Budget

SP: Special Publication