FDIC DIRECTIVE 1360.15

Access Control for Information Technology Resources

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

Originating Division/Office: Chief Information Officer Organization

Approval Date: 01/19/2023 **Pedestrian Change Date**: 09/26/2023

PURPOSE

This revised Directive provides policy and describes responsibilities for managing access control to FDIC Information Technology (IT) resources and associated data to protect its confidentiality, integrity, and availability.

SCOPE

This Directive applies to all FDIC Divisions/Offices requiring access to FDIC IT resources and information, such as FDIC networks, cloud platforms, applications, and shared files.

AUTHORITIES

See Appendix.

FORMS

- FDIC Form 1370/01, Verification of Computer-Based Resources Access Review
- FDIC Form 1370/02, Computer Access Authorization
- FDIC Form 1370/03, Application Workflow
- FDIC Form 1370/11, New, Transfer, or Detailed User Access Authorization

SUMMARY OF CHANGES

This Directive supersedes FDIC Circular 1360.15, Access Control for Automated Information Systems, dated March 31, 2011.

REVISION, dated January 19, 2023

This Directive had been revised to recognize cloud platforms and to provide guidance and associated responsibilities applicable to logical access control:

PEDESTRIAN CHANGE, dated September 26, 2023

This Directive had been revised to provide additional clarification to the Policy Section A.8 on the access removal of separated employees.

TABLE OF CONTENTS

PURPOSE 1
SCOPE 1
AUTHORITIES 1
FORMS 1
SUMMARY OF CHANGES 1
BACKGROUND 4
POLICY 5
A. Access Control 5
B. Disciplinary Action 6
RESPONSIBILITIES 7
A. Director, Division of Information Technology 7
B. IT Resource Owners 7
C. Information Security Managers 7
D. Authorized Users 8
E. Oversight Managers 8
APPENDIX 9
GLOSSARY OF TERMS 10
GLOSSARY OF ACRONYMS 11

BACKGROUND

The FDIC IT environment is comprised of various IT resources[1] that support the Corporation's mission. Authorized users require logical access to FDIC IT resources and information. Access to these resources must be appropriately controlled in order to protect the confidentiality, integrity, and availability of all associated data.

The use of IT resources is managed through authorized user accounts assigned to individuals, cloud platforms, applications, IT services, and automated processes. Granting access control provides an authorized user account the ability to take action within an IT resource, such as executing a program, using a service, and reading, updating, or deleting a file. Access control governs who is provided access and the type of actions allowed on the IT resource.

[1] IT resource include (but are not limited to): hardware computing platforms, the FDIC network, cloud platforms, databases, shared folders, applications, and software products.

POLICY

It is FDIC policy to provide guidance for access control that protects IT resources and information from unauthorized access, use, modification, disclosure, and destruction.

A. Access Control

1. Access controls are implemented whenever an IT resource owner requires access to an IT resource that must be restricted to a limited group of authorized users, or when authorized users require different types of access.

2. IT resources which are widely available to all authorized users (e.g., Internet access, office software) may not require any access controls.

3. Access to IT resources is provided for legitimate business use and only after proper authorization has been provided. Access is removed if the authorized user:

   a. Is assigned a change in job responsibilities;

   b. Transfers to a different organization; or

   c. No longer requires access.

4. A principle of least privilege for access is enforced. Authorized users are provided the minimal level of access required to allow them to perform their duties.

5. Access controls are used to enforce the principle of separation of duties, restricting the level of access provided to any single individual, when required.

6. Access may be granted through predefined roles. Assigning an authorized user account to a role provides it with a defined level of access to a distinct collection of IT resources.

7. A method for controlling access may be provided by an operating systems platform, built into the resource, through an Automated Information System or a third-party solution.

8. Access to IT resources remains active only while an authorized user is employed by the FDIC. Users do not have access before they begin work at the FDIC and access is terminated when it is no longer needed. Access may be disabled while an authorized user is away on extended leave.

9. Periodic reviews of access settings are conducted to ensure appropriate controls remain consistent with existing authorizations and current business needs.

B. 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; Directives 2410.6, Standards of Ethical Conduct for Employees, and 2750.1, Disciplinary and Adverse Actions; and applicable collective bargaining agreements.

RESPONSIBILITIES

A. Director, Division of Information Technology (DIT):

1. Develops, maintains, and enforces IT access control policy;
2. Provides overall guidance on IT access control issues;
3. Integrates and addresses IT access control through all phases of the systems development life cycle and procurement process for projects and systems;
4. Maintains systems to track access requests, authorizations, and resource owners;
5. Documents IT resources;
6. Provides an automated process for IT resource owners to conduct periodic reviews on access rights;
7. Assists in the resolution of IT access control conflicts and problems; and
8. Grants and revokes access to IT resources as authorized by IT resource owners.

B. IT Resource Owners:

1. Identify, document, and communicate to DIT all access requirements for IT resources for which they are responsible;
2. Participate in the development and testing of access requirements for application systems and cloud platforms supporting their Division/Office;
3. Authorize, as appropriate, all requests for access to IT resources for which they are the owner;
4. Authorize, as appropriate, the type and level of access to be granted to each authorized user; and
5. Conduct periodic reviews of access settings of which they are owners in order to ensure appropriate controls remain consistent with existing authorizations and current business needs as well as initiate corrective actions, as necessary, as a result of periodic reviews.

C. Information Security Managers:

1. Assist with identifying IT resource owners in their Division/Office and help IT resource owners carry out IT access control responsibilities;

2. Communicate IT access control issues to Division/Office management and DIT for resolution; and

3. Coordinate the performance of access reviews with IT resource owners and ensure reviews are completed and documented.

D. Authorized Users:

1. Comply with IT access control policy; and

2. Use the designated Automated Information System(s) maintained by DIT to request appropriate access to IT resources consistent with the principle of least privilege.

E. Oversight Managers:

Ensure contractors and subcontractors that are granted access to FDIC IT resources comply with all IT access control guidelines.

APPENDIX

External Authorities:

- Public Law 113-283, Federal Information Security Modernization Act of 2014
- Title 40, United States Code (U.S.C.), Subtitle III, Information Technology Management (Clinger-Cohen Act of 1996, as amended)
- Title 44, U.S.C., Chapter 35, Coordination of Federal Information Policy
- Executive Order 14028, Improving the Nation's Cybersecurity, dated May 12, 2021 [Least Privilege]
- Federal Information Processing Standards 200 - Minimum Security Requirements [Account Management]
- National Institute of Standards and Technology, Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations
- Office of Management and Budget, Circular A-130, Managing Federal Information as a Strategic Resource

Internal Authorities:

- FDIC Directive 1300.04, Information Technology Acceptable Use
- FDIC Directive 1310.03, Information Security Risk Management Program
- FDIC Directive 1360.01, Information Security Program
- FDIC Directive 1360.09, Protecting Information

GLOSSARY OF TERMS

Access Control: The process of granting or denying specific requests for obtaining and using information and related information processing services.

Authorization: Access privileges granted to an authorized user, program, or process or the act of granting those privileges.

Authorized Users: FDIC employees, contractor personnel, and others requiring logical access to FDIC IT resources and information.

IT Resource Owners: Employees identified by and representing an FDIC Division/Office, or their delegate, responsible for sponsoring, managing, and dictating access to a particular application, cloud platform, service, or file.

Least Privilege: A principle where authorized user accounts are provided the minimal, most restrictive set of permissions to an IT resource required to accomplish a task.

Logical Access: An authorized user's ability to access one or more computer system resources, such as a workstation, network, application, or database based on the validation of an individual's identity through some mechanism, such as a PIN, card, biometric, or other token, depending on the individual's roles and responsibilities in an organization.

Periodic Review: The evaluation of access rights to ensure appropriate controls remain consistent with existing authorizations and current business needs.

Role: A grouping of authorized user accounts with a common access requirement in which access may be assigned to a position rather than to each individual authorized user accounts. Examples include: employee, contractor, division, section, location, and job function.

Separation of Duties: A principle that involves limiting the ability of an authorized user account to complete only a portion of a function rather than the entire function in order to minimize the potential for fraud or error.

GLOSSARY OF ACRONYMS

DIT: Division of Information Technology

IT: Information Technology