*A pedestrian change has been made to the directive and appears in blue. – 3/31/2011

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.15	
CONTACT	TELEPHONE NUMBER
Todd A. Schotanus	(703) 516-5841
DATE	
February 27, 2009	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Employees and Contractors

FROM: Russell G. Pittman
Chief Information Officer

SUBJECT: Access Control for Information Technology Resources

1. Purpose

To issue revised policy and responsibilities for managing access to FDIC information technology (IT) resources and associated data.

2. Scope

The provisions of this circular apply to all FDIC employees, contractors, and others requiring logical access to FDIC IT resources and information, including computing platforms (e.g., network, mainframe, personal computer, and voice/video), applications, data, and shared files hosted internally by FDIC or externally by third parties on behalf of FDIC.

3. Revision and Cancellation

FDIC Circular 1360.15, Access Control for Automated Information Systems, dated September 24, 2003, is hereby revised and superseded.

FDIC Circular 1370.1, Periodic Review of Mainframe Resources Access, dated July 17, 1995, is hereby cancelled.

4. Background

The FDIC operates a number of hardware computing platforms and maintains a variety of applications and software products that comprise the IT resources that support the Corporation's mission. A fundamental information security principle requires that access to these resources be appropriately controlled in order to protect the confidentiality, integrity, and availability of the resource and all associated data.

The use of IT resources is managed by means of user accounts assigned to individuals, applications, IT services, and other automated processes. Providing *access* gives a user account the ability to take action with an IT resource (e.g., execute a program,

Background (cont'd)

use a service, read/update/delete a file). *Access control* governs both who is provided access and what type of actions they are allowed to perform on that resource.

Properly applied, access control protects IT resources and associated data from unauthorized access, use, modification, disclosure, and destruction. The Division of Information Technology (DIT) maintains systems for tracking access requests and authorizations, as well as procedures for reviewing access on a periodic basis.

5. Definitions

Terms specific to this circular are defined below:

a. **Access Control**. The means by which a user account is allowed or denied the ability to take action with an IT resource.

b. **Authorization**. The granting of permission to take action with an IT resource.

c. **IT Resource Owner**. Employee(s) identified by and representing the FDIC division/office responsible for sponsoring, managing, and dictating access to a particular IT resource such as an application, service, or file.

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

e. **Role**. A logical grouping of user accounts with a common access requirement so that access may be assigned to the role rather than to each of the individual user accounts. Examples of roles include employee, contractor, division, section, location, and job function.

f. **Separation of Duties**. A principle that involves limiting the ability of a user account to complete only a portion of a function rather than the entire function so as to minimize the potential for fraud or error.

6. Policy

In order to maintain control over access to IT resources, it is the policy of FDIC that:

a. Access controls shall be implemented whenever an IT resource owner requires that access to the IT resource must be restricted to a limited set of users or that different users require different types of access. IT resources that are widely available to all users (e.g., Internet access, office suite software, etc.) may not require any access controls.

Policy (cont'd)

b. Access to IT resources shall be provided for legitimate business use only and only after proper authorization has been provided when required. Access shall be removed if the job responsibilities of the user change, if the user transfers to a different organization, or if the user no longer requires access for any other reason.

c. The principle of least privilege for access shall be enforced. Users shall be provided the minimal level of access required to allow them to perform their duties.

d. Where required, access controls shall be used to enforce the principle of separation of duties to restrict the level of access and ability provided to any single individual.

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

f. The method for controlling access may be provided by an operating system platform, built into the resource, or through a third-party solution.

g. Access to IT resources shall remain active only while an individual is employed by or contracted to the FDIC. All access shall remain disabled prior to entering and shall be terminated immediately after exiting the FDIC. Access may be disabled while a user is away on extended leave.

h. Periodic reviews of access settings shall be conducted to ensure that appropriate controls remain consistent with existing authorizations and current business needs.

7. Responsibilities

a. Division/Office **IT Resource Owners** shall:

(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 supporting their division/office;

(3) Authorize (as appropriate) all requests for access to IT resources for which they are the owner consistent with the policy outlined in this circular;

(4) Authorize (as appropriate) the type/level of access to be granted to each authorized user consistent with the policy outlined in this circular;

Responsibilities (cont'd)

(5) Notify and coordinate with DIT any changes in IT resource access requirements;

(6) Review IT access settings periodically, consistent with risk to the resource and sensitivity of data, to verify that users and access levels are correct as authorized and reflect current business needs. Initiate corrective actions as necessary; and

(7) Serve as the point of contact for IT access control issues for IT resources for which they are responsible.

b. Division/Office **Information Security Managers (ISMs)** shall:

(1) Assist with identifying IT resource owners in their division/office and help them to carry out their 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 that these reviews are completed and documented.

c. **Division of Information Technology (DIT)** staff shall:

(1) Develop, maintain, and enforce corporate-wide IT access control policy;

(2) Provide overall guidance on IT access control issues;

(3) Integrate and address IT access control requirements through all phases of the systems development life cycle or procurement process for projects and systems;

(4) Maintain a system for tracking and documenting IT resources, resource owners, access requests, and authorizations;

(5) Grant and revoke access to IT resources as authorized by IT resource owners; and

(6) Assist in the resolution of IT access control conflicts and problems.

d. All **IT Resource Users** shall:

(1) Comply with IT access control policy as outlined in this circular; and

Responsibilities (cont'd)	(2) Utilize the system(s) maintained by DIT for requesting access to IT resources.
8. Additional Information	Questions regarding the provisions outlined in this circular should be addressed to the Supervisory IT Specialist, Security Policy & Compliance Section, DIT.
9. Effective Date	The provisions outlined in this circular are effective immediately.