* Pedestrian changes have been made to the directive and appear in blue. – 3/7/2012

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.10	
CONTACT	TELEPHONE NUMBER
Brian H. Seborg	(703) 516-1168
DATE	
February 27, 2003	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All FDIC Employees and Contractors

FROM: Russell G. Pittman
Chief Information Officer

SUBJECT: Corporate Password Standards

1. Purpose

To issue revised policy, standards, and responsibilities for creating and using secure passwords to access FDIC Automated Information Systems (AISs), and to address the changing and deleting of passwords.

2. Revision

FDIC Circular 1360.10, Corporate Password Standards, dated November 24, 1997, is hereby revised and superseded.

3. Scope

The provisions of this circular apply to all employees and non-FDIC personnel (e.g., employees of other government agencies and FDIC contractors) who have access to FDIC AISs.

4. Background

In the absence of more advanced access controls, passwords are the first line of defense to ensure that access to corporate data is limited to only authorized users. In FDIC's environment, passwords consist of a series of alphanumeric and special characters that are created and utilized by authorized users to gain access to FDIC AISs. The presence of well-constructed, frequently changed passwords can help limit access to corporate data to only those users who know the password. To achieve the most effective security levels, access to sensitive data protected by passwords is limited to users who use passwords in the proper way.

5. Policy

It is the policy of the FDIC that access to all FDIC AISs containing or potentially containing sensitive data and for which user accountability is required shall be granted only through the use of a valid and current password.

6. Password Standards

a. **Password Standards**. AISs requiring password protection shall only be accessed by password protected user accounts, including training and testing accounts. All passwords shall conform to the following standards:

(1) New user accounts shall be assigned random passwords that must be changed by the user immediately upon initial log-in.

(2) Users shall never give permission to another person to use their personal password, except as authorized for emergency procedures approved by the Director, Division of Information Technology (DIT).

(3) Passwords must have a minimum of eight characters. If an application/system does not allow passwords of at least eight characters, passwords shall be set to the maximum length allowed by the application/system.

(4) New or changed passwords must differ from the ten passwords previously established by a user.

(5) Passwords must contain characters from at least three of the following four categories:

- English uppercase letters (**A** through **Z**)
- English lowercase letters (**a** through **z**)
- Arabic numerals (**0** through **9**)
- Punctuation and other special characters (**! @ # $ % ^ & * ( ) _ + | ~ ` - = \ { } [ ] : ” ; ’ < > ? , . /**)

If an application/system cannot accommodate this requirement, it shall be configured to require the strongest level of password complexity possible within its configuration limitations.

(6) Passwords shall never be transmitted or displayed on a monitor, printed, or stored in plain text.

(7) Passwords must be changed after 90 days using the password expiration facilities. Passwords can be changed in less than 90 days, but shall not be changed by the user more frequently than once per day.

(8) An application’s/system’s account shall automatically be disabled if the account has not been accessed for a period of 120 days or for a period of time as specified by network or application policies.

(9) Accounts must be disabled for all position-specific applications/systems when the password owner is transferred

Password Standards (cont'd)

from his/her current position to another position within FDIC or upon termination of his/her employment or contract with FDIC.

(10) Password use must be monitored. Logs must be maintained for invalid log in attempts. Any failed log in attempt that deviates from the normal or accepted range of activity must be noted in an exception report.

(11) DIT shall prepare exception reports on a daily basis and make the reports available to the division's/office's Information Security Manager (ISM) for review.

(12) Password expiration warning messages for log in passwords shall be issued automatically to users at least five (5) calendar days before the password's expiration date.

(13) Passwords will be automatically disabled after five (5) consecutive unsuccessful user log-in attempts.

(14) Expired passwords can be reset by the user. Disabled or suspended passwords shall be reset by DIT.

(15) Evidence of password abuse or compromise must be reported as soon as known to the FDIC Computer Security Incident Response Team (CSIRT), as required by FDIC Circular 1360.12, Reporting Computer Security Incidents.

(16) Passwords must be changed immediately upon evidence of system abuse or user name/password compromise.

(17) Embedded or hard-coded passwords within systems, databases, and batch processes must be encrypted and approved by the Associate Director, Information Security and Privacy Staff (ISP), DIRM.

(18) Passwords must not be included in a macro or function key to automate log in.

(19) Passwords must be stored only as encrypted hash files.

b. **Exceptions**. If a user, for operational purposes, deems it essential to be exempted from the requirements of this circular, a Memorandum of Understanding (MOU) shall be executed by him/her to address any exceptions to the password standards identified in paragraph 6. a., above. The documentation supporting the request for an exception should include, at a minimum, background information; operational area(s) where there will be non-compliance; identification of risk as a result of non-compliance; a justification for the request; compensating controls; a petition for exception, etc. The Associate Director, ISP, DIT, is responsible for approving or disapproving all MOUs.

7. Definitions

Terms specific to this circular are defined below:

a. **Automated Information Systems (AISs)**. An application of information technology that is used to process, store, or transmit information and includes, but is not limited to, mainframe systems, mini/microcomputer systems, personal computers, gateways, private branch exchanges (PBXs), and networks that connect them and related software. AISs also include commercial and custom developed software, removable media, electronic and paper input documents, and output.

b. **Biometric**. Authentication techniques that rely on measurable physical characteristics that can be checked automatically. Examples include computer analysis of fingerprints or speech.

c. **Computer Security Incident Response Team (CSIRT)**. A team of computer professionals established by the FDIC to provide centralized, expeditious technical assistance to effectively investigate, resolve, and close security vulnerabilities and incidents involving FDIC AISs.

d. **Embedded/Hard Coded Passwords**. Passwords stored within the executable code or other application files.

e. **Encrypted Hash File**. A file containing user passwords that is transformed into a shorter fixed-length value, then translated into a form that is unintelligible.

f. **General Support Systems (GSSs)**. An interconnected set of information resources (as defined in Appendix III to OMB Circular No. A-130, Management of Federal Information Systems) under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communication, and people.

g. **Information Security Manager (ISM)**. An individual assigned to each division/office to ensure compliance with FDIC security directives, implement business specific security practices, and serve as primary liaison to DIT, ISP.

h. **Major Applications (MAs)**. Information technology applications that require special security attention due to the combined importance of their confidentiality, integrity, and availability to the FDIC.

i. **Memorandum of Understanding (MOU)**. A petition for a waiver by DIT of one or more FDIC Information Technology System Standards. MOUs originate in the division/office

Definitions (cont'd)

seeking the waiver and are approved/disapproved by the Associate Director, ISP, DIT. MOUs are typically granted once the petitioner has proven that adequate security controls are in place and additional risk associated with the waiver is acceptable.

j. **Password**. A protected, private character string used to authenticate an identity and to authorize access to data.

k. **Rules of Behavior.** Guidelines established for GSSs or MAs that hold users accountable for their actions and responsibilities for information security. Rules of behavior establishes standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program.

l. **Sensitive Data**. FDIC data that meets any of the following criteria (including data that resides and operates on personal computers, LANs, and FDIC mainframes):

(1) Data covered by the Privacy Act of 1974;

(2) Data or information protected from disclosure by any applicable statue, law, regulation, order, or privilege;

(3) Financial data used to produce checks; and

(4) Data considered essential or vital to FDIC operations that are susceptible to fraud or misuse in financial or procurement processes.

m. **Smartcard**. A small electronic device, about the size of a credit card, that contains electronic memory and an embedded integrated circuit. Smartcards are used for a variety of purposes, including storing a user's digital certificate and generating network IDs.

n. **System Administrator**. An individual responsible for maintaining a multi-user computer system, including a local area network.

o. **User Account**. Identification (sameness assurance) related to a user to ensure that the proper person is using a system/ application.

---

8. Responsibilities

a. **DIT, ISP** shall:

(1) Provide guidance and support to the FDIC regarding corporate password standards;

Responsibilities (cont'd)

(2) Provide opinions to DIT management concerning the adequacy of controls regarding password use for FDIC systems/applications;

(3) Assist ISMs with incident report monitoring and follow-up;

(4) Perform mainframe and Entrust password resets;

(5) Review and approve MOUs for embedded/hard coded passwords;

(6) Make rules of behavior available to employees as part of security awareness training;

(7) Develop emergency procedures for managing exceptions, which allow password usage in non-standard ways;

(8) Along with DIT, Infrastructure Services Branch (ISB), configure systems to comply with the provisions outlined in this circular or petition for MOUs seeking waivers for commercial systems that cannot comply;

(9) Work with DIT, ISB to disable user account(s) as soon as possible when notified of an employee's/contractor's termination or transfer; and

(10) Enable user accounts (ACF2) for new users.

b. **Divisions/Offices** shall:

(1) Establish or modify local procedures, application-specific rules of behavior, standards, and guidelines to ensure adherence to this circular;

(2) Ensure that all employees and contractors are aware of password management responsibilities;

(3) Assume responsibility for all password usage not in conformance with this policy through the use of MOUs granting waivers to this policy; and

(4) Take appropriate disciplinary action as outlined in the general support system or application-specific rules of behavior and FDIC policies.

c. **ISMs** shall:

(1) Check exception reports and conduct reviews, as necessary, to ensure compliance;

Responsibilities (cont'd)

(2) Contact the affected user to resolve password violations; and

(3) Coordinate incident follow-up with DIT, ISB.

d. **Supervisors, Contract Oversight Managers, DIT, ISP, in conjunction with Administrative Officers** shall:

(1) Request access for employees/contractors; and

(2) Support the Pre-Exit Clearance process for departing employees/contractors in accordance with FDIC Circular 1360.15, Access Control for Automated Information Systems and FDIC Circular 2150.1, Pre-Exit Clearance Procedures for FDIC Employees.

e. **DIT, ISB** shall:

(1) Along with DIT, ISP, configure systems to comply with this circular or petition for MOUs seeking waivers for commercial systems that cannot comply;

(2) Work with DIT, ISP, to disable user account(s) as soon as possible when notified of an employee's/contractor's termination or transfer; and

(3) Enable Windows user accounts for new users.

f. **DIT Help Desk** shall perform network password resets.

g. **Developers/Installers** shall:

(1) Comply with the password policy in all respects described herein to include custom developed applications or, if compliance cannot be met, petition DIT, ISP for a MOU seeking a waiver from this policy; and

(2) Petition for an MOU for any commercial off-the-shelf (COTS) product being considered that cannot comply with the requirements in this circular.

g. **FDIC Computer Users** shall:

(1) Complete all security awareness training addressing management of passwords;

Responsibilities (cont'd)

(2) Establish different passwords for each application/system (when applications/systems are not controlled through a "single sign-on" process), particularly when systems contain sensitive information;

(3) Change and reset passwords as required, and notify CSIRT if they suspect that any password has been compromised;

(4) Protect the confidentiality of passwords;

(5) Refrain from writing down passwords;

(6) Refrain from configuring hot-keys, speed-dial buttons on a telephone, terminal emulation software, or modem software to automatically log-in;

(7) Employ password-protected screensavers when leaving any computer unattended to which the user is logged on;

(8) Change system passwords as prompted by the system at least once every 90 days;

(9) Refrain from disclosing or sharing passwords, or from using another user's account (log in ID and password) to access a system, except as stated in paragraph 6. a. (2), above;

(10) Create and use secure passwords as documented in paragraph 9., below, when possible; and

(11) Notify DIT Help Desk of errors or problems associated with the log in process. If provided by the system, note the time, date, and location indicated for the previous sign on and inform the system administrator immediately if this information differs from that expected.

---

9. Additional Criteria for the Creation of Secure Passwords

It is imperative that passwords be well designed and properly implemented. The steps outlined below shall be followed to further protect against password break-in attempts:

a. Use both alphanumeric and special characters when designing passwords. Increasing the number of possible characters in each position makes the password harder to discover. If the password contains only letters, there are only 26 possibilities (52 possibilities if case distinctions are recognized) for each character in the password. If only numbers are used, there are only 10 possibilities for each character. If both letters

Additional Criteria for the Creation of Secure Passwords (cont'd)

(alpha) and numbers (numeric) are allowed, there are 36 possibilities for each character. To increase the complexity, use special characters (for example, @ and !) and mixed capitals and lower case letters when possible.

b. Create passwords that are at least eight characters in length. Some applications/systems may not permit an eight-character password. In such a case, use the maximum characters permitted by the system.

c. Choose a password that is memorable, but hard to guess. Make sure that it is NOT a name, a word, or something associated with an individual, such as log in ID, birth date, initials, children's names, a sport, etc. Ensure that the password is NOT related to a place of business or a project, and avoid keyboard related passwords such as "asdfjkl" or repeating sequences such as "111111" or "aaaaaaa."

d. Do not use English or foreign words preceded or terminated with a number or special character such as "Password1," "Andrea2," or "Redskins."

e. Choose passwords that are a combination of disassociated words, or compose a password from the first letters of a verse in a favorite poem or song. The following examples illustrate how a password could be composed: Ouamdw1p (once upon a midnight dreary while I pondered) or Ia#6wi#1? (I am number six who is number one?).

Note: Do **not** use any of these examples since they have been made public.

---

10. Disciplinary Action

Users who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to disciplinary action. Any disciplinary action shall be administered in accordance with applicable laws and regulations, including FDIC Circulars 2410.6, Standards of Ethical Conduct for Employees of the Federal Deposit Insurance Corporation (FDIC), and 2750.1, Disciplinary and Adverse Actions, and applicable collective bargaining agreements.

---

11. Questions

Questions pertaining to the provisions outlined in this circular should be referred to the Chief, Security Policy & Compliance Section, DIT.

---

12. Effective Date

The provisions outlined in this circular are effective immediately.