Acceptable Use Policy for FDIC Information Technology

PURPOSE
To provide FDIC policy on the limited personal and prohibited uses of the Corporation's Information Technology (IT).

SCOPE
The provisions of this Directive apply to FDIC employees, contractor personnel, and any other authorized users of FDIC IT services.

AUTHORITIES
- FDIC 1210.01, Records and Information Management Program
- FDIC 1360.9, Protecting Sensitive Information
- FDIC 1370.6, Communicating on Social Media Sites
- FDIC 3100.2, Guidelines for the Use of Voice Telecommunications Services
- FDIC 3100.4, Wireless Telephone and Pager Assignments, Usage, Safeguards, and Asset Management

FORM(S)
None

REVISION(S)
This Directive supersedes 1300.4, Acceptable Use Policy for Information Technology Resources, dated January 15, 2015. Upon approval, this Directive will be renumbered to 1300.04.
Summary of Changes (if applicable)

This Pedestrian Change updates the:

- Policy Section A.9 regarding the use of downloading data to removal devices by replacing the current manual process for approving the downloading of data to a removal device with an automated process using the FDIC's identity management system; and

- Responsibilities Section G.2 to include a new section for Supervisors to approve the request of their employees to obtain a removal device.
Table of Contents

Action Log.................................................................................................................................. 2
Summary of Changes (if applicable) .......................................................................................... 2
Table of Contents....................................................................................................................... 3
Background................................................................................................................................ 4
Policy ......................................................................................................................................... 5
  A. FDIC IT Resources ................................................................................................... 5
  B. IT Equipment at Financial Institutions ....................................................................... 6
  C. FDIC IT Equipment Configuration............................................................................. 6
  D. FDIC IT Equipment Connections .............................................................................. 6
  E. Professional Conduct ................................................................................................ 7
  F. Use of Personal Accounts and Devices .................................................................... 7
  G. Limited Personal Use ................................................................................................ 8
  H. Prohibited Use .......................................................................................................... 8
  I. Disclaimers ............................................................................................................... 8
  J. Monitoring ................................................................................................................. 9
  K. Privacy .....................................................................................................................10
  L. Disciplinary Action ...................................................................................................10
Responsibilities .........................................................................................................................11
  A. CIOO ....................................................................................................................... 11
  B. CIOO/Office of the Chief Information Security Officer ..............................................11
  C. CIOO/DIT ................................................................................................................11
  D. DOA/LERS ..............................................................................................................11
  E. Legal Division/Corporate Operations Branch ...........................................................11
  F. Legal Division/Deputy General Counsels ................................................................. 12
  G. Supervisors ..............................................................................................................12
  H. Authorized Users .....................................................................................................12
Appendix...................................................................................................................................13
Glossary of Terms.....................................................................................................................14
Glossary of Acronyms ...............................................................................................................16
Background

The FDIC invests a significant amount of capital to provide and maintain IT equipment and services ("resources") in support of the overall mission of the Corporation.

Supporting and protecting this investment in equipment and services requires implementing standards and enforcing rules governing use.

The Corporation’s acceptable use policy represents a significant component of the Corporation’s commitment to protect its IT resources and data from unauthorized, harmful, or inappropriate use by individuals, both inside and outside the Corporation.
Policy

The FDIC provides IT resources for the purpose of conducting official business in support of the FDIC’s mission. Authorized users of FDIC IT services are required to use these resources consistent with applicable policies.

A. FDIC IT Resources

1. Only authorized equipment and services furnished by the FDIC (or by contractor personnel if stated in the terms of the contract) may be connected to FDIC IT resources in an FDIC facility or at a financial institution. FDIC employees and contractor personnel, however, may connect mobile devices (e.g., smart phones, tablet computing devices, or laptop computers) that are not furnished by the FDIC to the “FDIC Guest Wi-Fi Network.”

2. Prospective vendors and external entities (e.g., individuals from other governmental entities) may connect personally owned, vendor-furnished, or agency-furnished mobile devices to the FDIC Guest Wi-Fi Network.

3. Students residing at the FDIC Student Residence Center at Virginia Square are authorized to use their personally owned equipment only for connecting to the FDIC Guest Wi-Fi Network.

4. Authorized users may use a personally owned audio “hands free” device with an FDIC furnished mobile device. The user of the hands free device must comply with applicable federal and state laws.

5. The FDIC has the right to remove unauthorized software or data from any FDIC equipment or service without notice to or consent of the user.

6. All FDIC sensitive information must be protected at the appropriate level for the level of sensitivity of the information. Employees, contractor personnel, and other authorized users of FDIC information systems must comply with FDIC 1360.9, Protecting Sensitive Information.

7. While performing business at a location other than an FDIC facility (e.g., teleworking), authorized users of FDIC IT resources are permitted to attach personally owned peripherals to an FDIC-furnished device. The personally owned peripheral must be configured to connect with FDIC furnished equipment in a manner that does not require any modifications to the FDIC-furnished device’s authorized settings (e.g., “plug and play” technology).
8. Solely for the purpose of importing data for the official use of the FDIC, a user may connect an external data storage device or insert a CD/DVD. Authorized users should exercise caution and, to the extent practicable, ensure the device is from a reputable source (e.g., an FDIC vendor, another government entity, a financial institution, a research institution, etc.).

9. Users are prohibited from downloading any data from any FDIC-furnished equipment to removable media (e.g., a USB storage device, CD/DVD, etc.). If there is a legitimate business need to do so, an exception may be granted by the CIOO, subject to the following:
   a. The device must be furnished by the FDIC and it becomes an accountable item;
   b. A request is submitted via the FDIC's identity management system with a justification and approved by the supervisor; and
   c. Approved exceptions require a recertification within six months of the last approval/recertification.

10. Use of FDIC IT resources in connection with Union-related representational functions is authorized.

11. Taking FDIC furnished IT equipment outside of the United States is prohibited unless otherwise authorized by the appropriate Division/Office Director. This authority may be delegated, in writing, to a subordinate executive manager within the same Division/Office. All approved requests to take FDIC IT equipment outside of the United States must be routed through the CIOO to ensure international service or to provision loaner equipment.

B. IT Equipment at Financial Institutions

Only FDIC-furnished or FDIC-authorized equipment may be used by authorized users for the performance of their official duties at financial institutions.

C. FDIC IT Equipment Configuration

Authorized users are allowed to make minor user preference settings modifications on FDIC furnished devices. However, unauthorized modifications (e.g., jailbreaking or rooting) an FDIC furnished device are strictly prohibited.

D. FDIC IT Equipment Connections

1. Without reconfiguring the FDIC furnished device, and subject to the other provisions in this Directive, authorized users may use an FDIC provided device to connect to:
a. Known and trusted internet services;

b. Personal cellular service providers (note: using the employee’s personal cellular service provider is at the expense of the employee unless explicitly authorized by other FDIC policies);

c. Cellular service providers via FDIC-issued cellular modems or FDIC provided Mi-Fi mobile hotspots;

d. A bank’s or other organization’s internet-accessible application(s) via the FDIC equipment’s browser software; or

e. A bank’s or other organization’s remote access services (excluding Virtual Private Network) as long as the other organization requires no administrative control over the FDIC equipment and the FDIC equipment does not become a node of the other organization’s network.

2. Although the use of public Hotspots and Wi-Fi is acceptable, the FDIC encourages authorized users to connect to the FDIC network through FDIC issued equipment and services.

E. Professional Conduct

Use of FDIC IT resources for communicating with others both inside and outside the Corporation must be conducted professionally.

F. Use of Personal Accounts and Devices

1. Except for phone calls, official FDIC business must be conducted using FDIC-provided equipment and FDIC email accounts. In the event of an emergency, non-FDIC-provided (e.g., personal) devices or personal email accounts may be used.

2. Employees and contractor personnel must use official FDIC email accounts for transmitting and receiving FDIC sensitive information. Employees are prohibited from using non-FDIC email accounts to transmit or receive FDIC sensitive information (e.g., Gmail, Hotmail, etc.).

3. Notwithstanding the general prohibition, if an employee or contractor personnel sends or receives a work related email or other communication on a non-FDIC furnished device or email account, the employee or contractor personnel must forward or “cc” such communication to the user’s own FDIC email account as soon as possible, but no later than 20 days after such sending or receiving occurs and must comply with the
requirements of 1210.01, Records and Information Management Program and the FDIC Records Retention Schedule.

G. Limited Personal Use

Use of FDIC IT resources is permitted subject to the following conditions:

1. Causes the FDIC no or negligible additional expense (e.g., paper, ink, electricity);
2. Avoids high bandwidth consumption and high cellular data usage, etc.; and
3. Complies with all applicable FDIC policies and user agreements.

H. Prohibited Use

Use of FDIC IT resources for the following activities is prohibited:

1. Performing any activity that is illegal under local, state, federal, or international law;
2. Operating a business;
3. Accessing, displaying, storing, or transmitting pornographic, sexually explicit, sexually oriented, violent, obscene, or indecent images or files;
4. Violating copyright, trademark, patent, trade secret, or licensing protections, including installing, running, or distributing “pirated” software or files;
5. Installing or using unauthorized software or services designed to share data or files or otherwise enable direct data sharing with other users, especially those outside the FDIC;
6. Interfering with security, which includes the confidentiality, integrity, and availability, of any computer system or IT service, internal or external to the FDIC, by causing intentional damage to or loss of data;
7. Engaging in text messaging, using either FDIC furnished or personally owned IT resources, while operating an FDIC owned, leased, or rented motor vehicle; and
8. Engaging in text messaging while operating a privately owned vehicle on official FDIC business.
9. Accessing any FDIC networks (e.g., the “Production” network) from a personally owned device, except for the FDIC Guest Wi-Fi network.

I. Disclaimers
All authorized users should recognize that their FDIC email address associates them with the FDIC. Those who participate in electronic forums (e.g., discussion groups, listservs, or news groups) and those who send emails containing personal opinions may have their comments mistaken as FDIC policy. Consequently, one should make appropriate disclaimers to avoid any such mistake.

J. Monitoring

FDIC IT resources are monitored by the FDIC for all lawful purposes. All information (including personal or confidential information) placed on or sent over an FDIC information system may be examined, recorded, copied, used, or disclosed by the FDIC for legitimate business purposes. All information collected during monitoring may be used for purposes of any administrative, civil, or criminal action or proceeding.

1. All requests for access to content of electronic information regarding any potential administrative or adverse personnel action must be approved by the following:
   a. Division of Administration (DOA), Assistant Director, Labor and Employee Relations Section (LERS),
   b. Legal, Assistant General Counsel, Labor, Employment, and Administration Section (LEAS), and
   c. Chief Information Officer Organization (CIOO), CISO.

2. All E-Vault searches for electronic discovery purposes in litigation, Freedom of Information Act requests, and Congressional requests must be approved by the Deputy General Counsel (responsible for the relevant subject area) and also approved by the Chief Information Security Officer.

3. Unless authorized to do so as part of their job function, individual users are not permitted to monitor or to disrupt the monitoring of IT resources, including all electronic communications.

4. Content

The FDIC reserves the right to monitor all IT resources and electronic communications, including content. Monitoring usually occurs when:

   a. The monitoring is necessary for non-investigatory purposes, such as troubleshooting an email problem by observing the message as it is transmitted;
b. There are reasonable grounds for believing that the monitoring may turn up evidence that an employee or contractor personnel has or is engaged in work-related misconduct or prohibited activities referenced in Prohibited Use;

c. There is a legal requirement for FDIC records to be examined or produced, such as those pursuant to Freedom of Information Act requests, congressional requests, court rules of procedure, or court orders; or

d. Emergencies involving internal security concerns that reasonably necessitate such monitoring.

5. The FDIC does not intend to monitor the content of electronic communications relating to Union representational activities. Should the content of any such communication be revealed, it shall be treated as confidential absent a legitimate business purpose.

6. Statistical Data

The FDIC collects and maintains statistical data concerning the support and maintenance of FDIC IT resources. While this data does not include specific content, it does include such things as location, size, and age of data files, origin, destination, and duration of electronic communications, and details regarding internet activity.

K. Privacy

Users have no expectations of privacy with regard to their use of FDIC IT resources. While the FDIC is committed to respecting individual privacy concerns consistent with applicable law, regulation, and policy, the Corporation has a duty to maintain and protect its IT resources.

L. Disciplinary Action

1. Authorized users who violate the provisions of this policy may be subject to disciplinary action up to and including removal from federal service or from their contract. Any disciplinary action will be administered in accordance with applicable law, regulations, FDIC policies and procedures, contractual agreements, and applicable collective bargaining agreements.

2. Persons or entities that access or use FDIC IT resources without authorization or contrary to law may be subject to criminal prosecution. In cases involving improper use of an IT resource, records produced through system monitoring and recording may be used as evidence for disciplinary actions and may be provided to law enforcement officials.
Responsibilities

A. CIOO

1. Provides and maintains IT resources for the use of FDIC employees, contractor personnel, and any other authorized users (except when specifically stated otherwise in a contract);

2. Authorizes, configures, installs, and uninstalls all software on FDIC equipment;

3. Provides assurances that FDIC IT resources are adequately protected from misuse, abuse, damage, and loss of availability;

4. Maintains this Directive on permitted and prohibited uses of IT resources;

5. Provides encryption capabilities to secure FDIC information; and

6. Communicates to the user how to adhere to this Directive.

B. CIOO/Office of the Chief Information Security Officer

CIOO/Office of the Chief Information Security Officer is responsible for providing assistance, as described in Monitoring, with requests for electronic communications data.

C. CIOO/DIT

CIOO/DIT is responsible for issuing and tracking all removable media devices that are approved (under the provisions contained in this Directive) for downloading information from an FDIC IT resource.

D. DOA/LERS

DOA/LERS is responsible for complying with Monitoring concerning requests by FDIC supervisors who are seeking to obtain electronic communications data regarding a specific employee.

E. Legal Division/Corporate Operations Branch

Legal Division/Corporate Operations Branch is responsible for complying with Monitoring concerning requests by FDIC supervisors who are seeking to obtain electronic communications data regarding a specific employee.
F. Legal Division/Deputy General Counsels

Legal Division/Deputy General Counsels are responsible for complying with Monitoring concerning requests for electronic discovery purposes in litigation, Freedom of Information Act requests, and Congressional requests.

G. Supervisors

1. Comply with the previous section on Monitoring when seeking to obtain electronic communications data for a specific employee.

2. Approve requests for removable media via the FDIC's identity management system, when there is a legitimate business requirement.

H. Authorized Users

All authorized users of FDIC IT resources are responsible for complying with the policy outlined in this Directive.
Appendix

None
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Users</td>
<td>Employees, contractor personnel, and any other authorized individuals who use FDIC information technology (IT) resources</td>
</tr>
<tr>
<td>FDIC Facility</td>
<td>Any FDIC controlled workspace or building</td>
</tr>
<tr>
<td>Information Technology Services</td>
<td>The application of business and technical expertise to enable FDIC to create, manage, optimize, or access to information and business processes using electronic mail, voice/video services, internet access, outsourced services, etc., including:</td>
</tr>
<tr>
<td>IT Resources</td>
<td>Any FDIC provided IT equipment or IT service</td>
</tr>
<tr>
<td>Jailbreaking (Rooting)</td>
<td>The removal of software restrictions imposed by an operating system or other security mechanism</td>
</tr>
<tr>
<td>Mi-Fi</td>
<td>Mobile Wi-Fi hotspot</td>
</tr>
<tr>
<td>Public Hotspots</td>
<td>Use of Wi-Fi as follows:</td>
</tr>
<tr>
<td></td>
<td>- Guest networks at hotels (both wireless and wired systems), banks, and business centers;</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Open wireless access</td>
<td>- Open wireless access at cafes, restaurants, bars, public areas, etc.;</td>
</tr>
<tr>
<td>Mobile hotspots</td>
<td>- Mobile hotspots (other than FDIC provided);</td>
</tr>
<tr>
<td>Unsecured wireless</td>
<td>- Unsecured wireless networks; or</td>
</tr>
<tr>
<td>Any wireless network</td>
<td>- Any wireless network access that the FDIC or the authorized user does not directly control.</td>
</tr>
</tbody>
</table>

**Sensitive Information**

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled (See 1360.9, Protecting Sensitive Information).

**Text messaging**

The act of reading from or entering data into any handheld or other electronic device and includes texting, emailing, instant messaging, etc.
### Glossary of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CIOO</td>
<td>Chief Information Officer Organization</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LEAS</td>
<td>Labor, Employment, and Administration Section</td>
</tr>
<tr>
<td>LERS</td>
<td>Labor and Employee Relations Section</td>
</tr>
</tbody>
</table>