Pedestrian Changes were made on 4/21/16 and are shown in blue.

FEDERAL DEPOSIT INSURANCE CORPORATION

# DIRECTIVE SYSTEM

| TYPE AND NUMBER | |
|---|---|
| Circular 1300.4 | |
| CONTACT | TELEPHONE NUMBER |
| Brian Seborg | (703) 516-1168 |
| DATE | |
| January 15, 2015 | |
| DATE OF CANCELLATION *(Bulletins Only)* | |

**TO**: All Employees and Contractors

**FROM**: Lawrence Gross Jr.
Chief Information Officer
Chief Information Officer Organization

**SUBJECT**: Acceptable Use Policy for Information Technology Resources

## 1. Purpose

To provide FDIC policy on the limited personal and prohibited uses of the Corporation's information technology (IT) resources.

## 2. Revision

FDIC Circular 1300.4, Acceptable Use Policy for Information Technology Resources, dated December 21, 2010, is hereby revised and superseded.

## 3. Scope

The provisions of this Circular apply to all users (employees, contractors, and other clients) of FDIC IT resources. IT resources include all FDIC-provided:

a. Hardware (e.g., desktop/laptop computers, telephones, and storage devices);

b. Mobile devices (e.g., tablet computers, personal digital assistants (PDAs), cameras, and mobile telephones);

c. Office equipment (e.g., printers, facsimile (fax) machines, scanners, and copiers/eCopy units);

d. Software, applications and outsourced information services; and

e. Services (e.g., electronic mail [email; including FDIC-issued email addresses], voice/video services, and Internet access).

This Circular also applies to personally-owned computers and devices used to access or transmit FDIC data, connect to FDIC resources, or to conduct FDIC business.

## 4. Background

The FDIC invests a significant amount of capital to provide and maintain IT equipment and services that improve business processes, increase productivity, and support the overall mission of the Corporation.

Supporting and protecting this investment in equipment and services requires that configuration standards be implemented and rules governing use be enforced. As technology has become integrated into normal operations, any disruption to the performance or availability of these resources can have significant impact on the accomplishment of FDIC's mission.

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

## 5. Policy

The FDIC provides IT equipment and services for official business purposes in support of the FDIC's mission. Employees and contractors are encouraged to use these resources in the performance of their job functions. It is FDIC policy that:

a. **IT Equipment and Services connected to FDIC Networks**. Only authorized equipment and services furnished by the FDIC (or by a contractor if stated in the terms of the contract) shall be connected to FDIC voice and data networks. Users shall not attach or connect any unauthorized services or personally-owned devices to the network (by wire or wireless). This includes, but is not limited to, desktops, laptops, tablets, printers, servers, routers, switches, hubs, network or traffic capture devices, outsourced information services, removable media (e.g., CD/DVDs, floppy diskettes, universal serial bus (USB) storage devices, zip drives, or other similar devices), smartphones, or video systems.

**Exception**: "Internet Only" Wi-Fi service is provided at some FDIC locations. Users who connect to the "Internet Only" Wi-Fi with a personally-owned device will be allowed access to resources available via the Internet.

(1) Users may only copy FDIC business related information onto a device or service authorized by the FDIC.

(2) Contractors, vendors, and visitors may use the "Internet Only" Wi-Fi service for non-FDIC communications.

**Policy (cont.)**

b. **IT Equipment at Financial Institutions.** Only FDIC-furnished or FDIC-authorized equipment shall be used by employees and contractors at financial institutions during on-site examination and/or on-site resolution activities.

**Exception**: Employees and contractors may bring and use personal cell phones for personal use. Personal cell phones may be used for business-related calls; however such use is at the employee's discretion and cost.

c. **FDIC IT Equipment Configuration**. Users shall not attempt to reconfigure FDIC equipment settings or configurations.

d. **FDIC IT Equipment Connections**. Users shall not attempt to use FDIC equipment to login to another organization's network such as a bank's internal network. Without reconfiguring it, the FDIC laptop may be used to connect to:

(1) Secured home Internet services;

(2) Cellular service providers via FDIC-issued cellular modems;

(3) A bank's or other organization's Internet-based application(s) via the FDIC equipment's browser software; or

(4) A bank's or other organization's network via remote access services (excluding Virtual Private Network (VPN)) provided by that organization, as long as the other organization requires no administrative control over the FDIC equipment.

Due to the inherent vulnerable nature of wireless, FDIC discourages the use of public "hotspots" or "Wi-Fi" to access the FDIC network. In the event that users must use public hotspots, users should always use FDIC approved remote access (i.e., RCN or FastAccess) when accessing business sensitive data, PII, or FDIC applications that require login information. Public "hotspots" or "Wi-Fi" may include, but are not limited to:

(1) Guest networks at hotels, banks, and business centers;

(2) Open wireless access at cafes, restaurants, bars, public areas, etc.;

(3) Mobile hotspots;

(4) Unsecured wireless networks; or

(5) Any wireless access that you do not have direct control over.

**Policy (cont.)**

e. **Personally-owned Accessories and Peripherals**. Users shall not attach or connect personally-owned accessories or peripherals to FDIC-furnished equipment.

**Exception 1**: Laptops or other mobile devices used in training classrooms or conference rooms to make presentations may be connected to overhead projectors.

**Exception 2**: Users may attach or connect a personally-owned individual printer or second monitor to FDIC-furnished equipment under the following conditions:

(1) No additional configuration of the FDIC-furnished equipment or installation of software drivers is required. Compatibility of personally-owned devices with current or future FDIC equipment is not implied or guaranteed;

(2) FDIC will not provide support for installing, troubleshooting, repairing, uninstalling, or disposing of personally-owned devices;

(3) FDIC will not provide ink or toner supplies for personally-owned printers. Personally-owned storage devices may be destroyed by placing them in electronic media consoles provided by the Corporation for this purpose;

(4) Personally-owned printers and monitors in the FDIC workplace shall be clearly marked as personal. Proof of ownership such as a purchase receipt shall be retained and provided upon request.; and

(5) No FDIC data will be downloaded to, or stored in, non-volatile memory (i.e., memory that is retained after the device is turned off) of the printer or monitor.

f. **Personally-owned Computers and Mobile Devices**. Personally-owned computers and mobile devices may be used to access FDIC applications, data, and resources for business purposes only through remote access services provided and supported by FDIC subject to limitations addressed in sections 5.b. and 5.c., above.

Users may connect personally-owned computers to the Internet from the Virginia Square Student Residence Center or other FDIC-provided guest networks as these networks are separated from the FDIC Corporate network.

g. **Activating Wireless Connectivity**. Only FDIC-authorized equipment providing wireless access to FDIC IT resources shall be activated in the FDIC workplace (which includes FDIC offices

**Policy (cont.)**

and open/closed financial institutions). Users shall not install any router or similar technology, or enable wireless hotspots on mobile devices in the FDIC workplace.

h. Use of FDIC IT resources such as phone systems, email, and Internet connectivity for communicating with others both inside and outside the Corporation shall be conducted professionally, and should not disparage the FDIC.

i. Email messages containing sensitive information shall always be encrypted using an FDIC-approved encryption product or service. Non-FDIC email accounts (e.g., Gmail, Hotmail, etc.) must never be used for transmitting or receiving any type of sensitive FDIC information without prior approval from their Contracting Officer or Supervisor and subsequent concurrence from the Chief Privacy Officer (CPO).

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

k. The lists below are not exhaustive, but attempt to provide a framework of activities which fall into the categories of limited personal use and prohibited use of FDIC IT resources:

(1) **Limited Personal Use**. Limited personal use of FDIC IT resources is permitted subject to the following conditions:

(a) Causes FDIC no or negligible additional expense (e.g., paper, ink, electricity, ordinary wear and tear, etc.);

(b) Generally occurs during non-work time (before or after scheduled work hours or during lunch or authorized breaks);

(c) Does not interfere with any official FDIC business activity;

(d) Does not impact IT resource capacity, performance, or productivity;

(e) Complies with all applicable FDIC IT Circulars; and

(f) Primarily involves only end-user equipment such as desktop/laptop computers, telephones, copiers, facsimile machines, etc.

Examples of acceptable limited personal use includes composing letters or developing spreadsheets for personal use, making or receiving personal telephone calls, copies, or faxes, sending and receiving personal emails, or browsing

**Policy (cont.)**

websites on the Internet, as long as these activities meet the conditions regarding limited personal use stated in this Circular.

**Note**: Users should expect only a minimum level of technical support in troubleshooting any problems experienced while using IT resources for personal use.

(2) **Prohibited Use**. Use of FDIC IT resources for the following activities is prohibited:

(a) Performing any activity that is illegal under local, state, Federal, or international law;

(b) Carrying out any activity that is malicious or fraudulent in nature;

(c) Operating a business, unauthorized fund-raising, or endorsing a product or service;

(d) Accessing, displaying, storing, or transmitting pornographic, sexually explicit, sexually oriented, violent, obscene, or indecent images or files;

(e) Violating copyright, trademark, patent, trade secret, or licensing protections. This includes installing, running, or distributing "pirated" software or files;

(f) Installing or using personally-owned or other unauthorized software (including screen saver and Internet toolbar software) or removing/disabling any authorized software. Installing or downloading non-work related music or video files to any FDIC network storage device or service. Additionally, the FDIC has the right to remove unauthorized data from any FDIC equipment or service without notice to or consent of the user;

**Exception:** Employees may load personal image files (e.g., family photos) for use as background "wallpaper," as long as they adhere to all other provisions of this Circular.

(g) Installing or using non-FDIC software designed to share data or files or otherwise collaborate directly with other users, especially those outside FDIC. Examples include, but are not limited to:

1. Peer-to-peer file sharing software used for distributing, sharing, sending, or receiving audio, video, or data files;

**Policy (cont.)**

2. Instant Messaging (IM) and Video Messaging programs used to send and receive real-time online chat and video messages between users; and

3. Groupware technology that allows for a collection of users to directly collaborate, communicate, and share data between and among their individual computers.

**Note**: Software, programs and technology intended for sharing or collaboration is allowed for internal use (among FDIC users) when provided and supported by the FDIC.

(h) Using FDIC IT communication services for:

1. Sending unsolicited commercial or advertising material (spam) or repeated, unwanted communication of an intrusive nature;

2. Initiating or propagating chain letters or other mass mailings;

3. Making statements that are profane, obscene, abusive, or intolerant of race, creed, color, ethnicity, national origin, disability status, sex, age, religious beliefs, or sexual orientation;

4. Making statements that slander or libel any individual or group; or

5. Harassing, annoying, threatening, or creating a hostile work environment for others.

(i) Using authorized access to FDIC systems or outsourced services to "snoop" or obtain information about anyone or anything without a legitimate business need to know.

(j) Engaging in text messaging while:

1. Driving an FDIC-owned, FDIC-leased, or FDIC-rented vehicle;

2. Driving a privately-owned vehicle while on FDIC business; or

3. Using FDIC-supplied equipment while driving.

**Note**: "Text messaging" means reading from or entering data into any handheld or other electronic device and includes texting, emailing, instant messaging, and

**Policy (cont.)**

obtaining navigational information. "Driving" means operating a motor vehicle on an active roadway with the motor running, including while temporarily stationary because of traffic, a traffic light, or a stop sign. It does not include operating a motor vehicle while stopped on the side of, or off of, an active roadway at a location where you can safely remain stationary.

(k) Hosting a personal website;

(l) Playing games or gambling;

(m) Engaging in political or lobbying activities;

(n) Promoting a social, religious, or political cause; and

(o) Interfering with the security, which includes the confidentiality, integrity, and availability, of any computer system or IT service, internal or external to FDIC, by:

1. Attempting to circumvent or compromise security to gain unauthorized access;

2. Distributing computer viruses, worms, Trojan horses, or trap-door programs;

3. Causing intentional damage to or loss of data;

4. Participating in activities that promote computer crime or misuse, including, but not limited to, posting or disclosing passwords, credit card and other account numbers, and system vulnerabilities;

5. Altering voice/data routing patterns or intentionally intercepting or re-routing network traffic;

6. Using tools or utilities to scan, probe, change, or attack a network (unless authorized to do so on FDIC's network in the course of testing or auditing security settings);

7. Using software cleaning utilities to delete, remove, cover-up, hamper, and/or camouflage information of evidentiary value in response to an FDIC investigation; or

8. Performing other computer "hacking" activities.

The Corporation's response to a violation of these prohibited uses will be applied in a common sense manner.

**Policy (cont.)**

l. **Disclaimers**. All users should recognize that their FDIC email address associates them with FDIC. Those who participate in electronic forums such as discussion groups, listservs, or news groups, and those who send emails containing personal opinions may have their comments mistaken as FDIC policy.

Whenever expressing any personal opinion that may be mistaken for FDIC policy, users shall add a disclaimer to any such communication. An example of a disclaimer is "The opinions expressed here are my own and do not represent official policy of the FDIC."

m. **Monitoring**. The FDIC monitors the use of all IT resources, including, but not limited to, telephone, email, and Internet services as well as the configuration and use of computer software and hardware. Monitoring may range from gathering general statistical information on usage for the purpose of maintaining and troubleshooting a system to examining the content of a specific file or data/communications transmission. By accessing FDIC's IT systems and using IT resources, users consent to this monitoring.

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

(1) **Content**. The FDIC reserves the right to monitor the content of all IT resources, including electronic communications. 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 has or is engaged in work-related misconduct or prohibited activities outlined in subparagraph 5.k.(2), above;

(c) It is necessary in order to comply with legal requirements that FDIC records be examined or produced, such as those of the Freedom of Information Act, court rules of procedure, or court orders; or

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

**Note**: The FDIC does not intend to monitor the content of any electronic communications relating to Union representational activities. Should any such content be

**Policy (cont.)**

revealed, it shall be treated as privileged, confidential, and shall not be disseminated.

**Statistical Data**. In its ongoing support and maintenance of IT resources, the FDIC collects and maintains statistical data regarding its use. 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.

(2) **Access to Monitoring Information**. Supervisors who wish to obtain electronic communications data regarding a specific employee or contractor must provide written justification and obtain written approval from an Executive-level Manager within their Division/Office. Approved justifications shall be forwarded to the Division of Information Technology (DIT) Deputy Director, Infrastructure Services Branch, for action.

Employees involved in complying with legal requirements pursuant to 12 C.F.R. Part 309 for the review or production of agency records must obtain written approval as provided in 12 C.F.R. Part 309 from their Division/Office Executive-level Manager and from the Corporation's General Counsel or his/her designee, except in the case of the Office of Inspector General, where approval must be obtained from the Counsel to the Inspector General or his/her designee. When required for processing access to FDIC IT resources, these approvals shall be forwarded to the DIT Deputy Director, Infrastructure Services Branch, for action.

n. **Privacy**. Users shall have no expectations of privacy with regard to their use of FDIC IT equipment and services. While the FDIC is committed to respecting the privacy concerns of the user community consistent with applicable law, regulation, and policy, the Corporation has a duty to maintain and protect its IT resources.

**6. Responsibilities**

a. **All Users** of IT resources are responsible for complying with the policy outlined in this Circular.

b. **CIOO** is responsible for:

(1) Providing and maintaining IT equipment and services for the use of FDIC employees and contractors (except when specifically stated otherwise in a contract);

(2) Authorizing, configuring, installing, and uninstalling all software on FDIC equipment;

| | |
|---|---|
| **Responsibilities (cont.)** | (3) Providing assurances that FDIC IT resources are adequately protected from misuse, abuse, damage, and loss of availability; and<br><br>(4) Maintaining this policy on permitted and prohibited uses of IT resources. |
| **7. Disciplinary Action** | Employees or contractors 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.<br><br>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 resources, records produced through system monitoring and recording may be used as evidence for disciplinary actions and may be provided to law enforcement officials. |
| **8. References** | References regarding the use of various IT resources are available in the following circulars:<br><br>a. FDIC Circular 1380.4, FDIC's Policy on the Use of Personal Digital Assistants (PDAs).<br><br>b. FDIC Circular 3100.2, Guidelines for the Use of Voice Telecommunications Services.<br><br>c. FDIC Circular 3100.4, Wireless Telephone and Pager Assignments, Usage, Safeguards, and Asset Management.<br><br>d. FDIC Circular 3120.1, Guidelines for the Distribution, Management and Usage of Facsimile Machines and Services.<br><br>e. FDIC Circular 1370.6, Communicating on Social Media Sites. |
| **9. Questions** | Questions regarding the provisions outlined in this circular should be addressed to the Chief, Policy and Compliance Section, Information Security and Privacy Staff, Chief Information Officer Organization. |
| **10. Effective Date** | The provisions outlined in this Circular are effective immediately. |