FDIC DIRECTIVE 1300.04

Information Technology Acceptable Use

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

Originating Division/Office: Chief Information Officer Organization

Approval Date: 01/12/2023

PURPOSE

This revised Directive provides policy on the limited personal and prohibited uses of the Corporation's Information Technology (IT).

SCOPE

This Directive applies to all FDIC Divisions/Offices.

AUTHORITIES

See Appendix.

FORMS

None.

SUMMARY OF CHANGES

This Directive supersedes FDIC Directive 1300.04, Acceptable Use Policy for FDIC Information Technology, dated November 16, 2020.

REVISION, dated January 12, 2023

This Directive has been revised to:

- Include applicable external authorities and additional internal authorities;
- Remove references to locations (e.g., the Student Residence Center) when referring to the FDIC Guest Wi-Fi Network;
- Exclude the authorization of IT resource use for confidential materials;
- Include policy for the use of non-FDIC IT resources at financial institutions;
- Revise policy regarding the sources of connection for FDIC-issued IT resources;

- Include additional policy regarding professional and ethical conduct when using FDIC-issued devices;
- Include exceptions for the use of non-FDIC accounts;
- Include additional examples of limited personal use and prohibited use;
- Provide policy for access to personal data saved on FDIC IT resources;
- Include policy regarding OIG access and monitoring responsibilities;
- Remove procedural language on statistical data;
- Revise responsibilities for the Chief Information Officer (CIO), Chief Information Security Officer, Legal Division, Supervisors/Managers, and Authorized Users;
- Include responsibilities for Contracting Officers and Oversight Managers; and
- Include additional terms and definitions in the Glossary.

TABLE OF CONTENTS

BACKGROUND

The FDIC invests a significant amount of capital to provide and maintain IT 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.

This Directive represents a significant component of the Corporation's commitment to protect its IT resources and data from unauthorized, harmful, or inappropriate use, both inside and outside the Corporation.

POLICY

The FDIC provides IT resources to conduct official business in support of the Corporation's mission. Authorized users of FDIC IT equipment and services are required to use these IT resources consistent with the applicable policies. The following requirements apply to all authorized users who use and access FDIC IT resources.

IT resources that are covered by this policy include all technology provided by the FDIC (e.g., computer systems, communications networks, and FDIC-furnished IT equipment, such as hardware or mobile devices and cloud or other outsourced technology used by the FDIC) and electronically stored information, including Corporate-related work products (which are the property of the Corporation and not the individual).

A. IT Resources

1. Only authorized equipment and services may be used by authorized users for the performance of official duties.

2. Subject to the provisions in this Directive, authorized users may use FDIC-issued IT resources to connect to:

    a. Personal cellular service providers (using the authorized user's personal cellular service provider is at the expense of the authorized user unless authorized by other FDIC policies);

    b. FDIC provided mobile hotspots;

    c. Internet-accessible application(s) via the FDIC equipment's browser software; or

    d. Remote access services (excluding the Virtual Private Network) as long as the other organization requires no administrative control over FDIC equipment and the FDIC equipment does not become a network node of the other organization's network.

3. Making minor user preference setting modifications on FDIC-furnished devices is permitted for authorized users. Unauthorized modifications (e.g., attempted jailbreaking or rooting) to an FDIC-furnished device are prohibited.

4. Authorized users and FDIC visitors, as defined in FDIC Directive 1610.01, Physical Security Program, are permitted to use personal IT resources to connect to the FDIC Guest Wi-Fi Network.

5. Access to Public Hotspots should be limited to password-protected sites and is permissible when Internet services are unavailable or limited to perform work on FDIC-issued equipment.

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

7. Only FDIC-approved solutions to host meetings to conduct official FDIC business are authorized.

8. Taking FDIC-furnished IT equipment outside of the United States (U.S.) and its territories[1] for official FDIC business is only permitted when authorized by the appropriate Division/Office Director. All approved requests to take FDIC IT equipment outside of the U.S. must be routed through the CIOO to ensure international service or to provision loaner equipment.

9. Use of FDIC IT resources in connection with Union-related representational functions is authorized, excluding confidential Corporate-related management materials.

10. All appropriately classified and categorized FDIC sensitive data and information must be protected per level of sensitivity, value, and criticality. Authorized users of FDIC information systems must comply with FDIC policy on protecting sensitive information in accordance with FDIC Directive 1360.09, Protecting Information.

11. Users are prohibited from downloading any FDIC-information to removable media (e.g., a USB storage device, CD, or DVD). An exception may be granted if there is a legitimate business need to do so, subject to the following:

    a. The device or media must be furnished by the FDIC and becomes an accountable item;

    b. The Division/Office Director, or designee, of the requesting authorized user determines there is a legitimate business requirement and recommends approval; and

    c. The CIO, or designee, approves the request. Approved exceptions expire within six months of approval or as otherwise deemed appropriate by the CIO.

B. Use of Personal Equipment

1. Except for phone calls, official FDIC business must be conducted using FDIC-provided equipment and email accounts over FDIC-provided remote access portals. FDIC information must never be saved or stored in personally-owned computers or devices.

[1] U.S. Territories include: American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands.

Non-FDIC-provided email accounts with supervisory approval may be used in the event of an emergency (see Use of Personal Accounts)

2. Authorized users of FDIC IT resources are permitted to attach personally owned peripherals (e.g., headphones, speakers, mice, keyboards, and monitors) to FDIC-furnished equipment. Personally owned peripherals 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).

3. 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.

4. Non-FDIC-furnished IT resources may be used by authorized users to connect and use FDIC-limited applications and services remotely via the Internet through designated FDIC Remote Access systems or approved Virtual Desktop Interfaces.

C. Use of FDIC Accounts

1. Electronic Messages and voice messages should only be used for internal communications that are logistical or administrative, such as scheduling or status inquiries. They are not records repositories and may not be used to record the decisions, actions, or strategies of the FDIC. Authorized users are required to transfer the content of any such messages (as well as voicemail generated by a software platform [e.g., electronic mail]) to a recordkeeping system if decisions, actions, or strategies of the FDIC have not been documented elsewhere in accordance with the email retention policy as described in FDIC Directive 1210.01, Records and Information Management Program.

2. In the event a voicemail or an audio or video conference includes a decision or action of the FDIC that has not been documented elsewhere, content of the decision or action must be maintained in accordance with the email retention policy as described in FDIC Directive 1210.01, Records and Information Management Program.

D. IT Equipment at Financial Institutions

Only FDIC-authorized IT resources are permitted to connect to and access FDIC-limited applications. Non-FDIC IT resources may be used by authorized personnel for the performance of their official duties at financial institutions.

E. Professional Conduct

Authorized users must comply with this Directive, including demonstrating professional and ethical conduct, in all forms of communication when using FDIC-issued devices, including mobile devices. This includes the use of downloaded apps, messaging apps, camera, and video recording capabilities. It also applies to email and the use of platforms that support collaboration and communication.

FDIC IT resources are subject to rules governing limited personal use, consistent with FDIC Form 1370/08, Request for Wireless Services, and FDIC Directives 1370.09, Assignments, Usage, and Safeguards of Mobile Devices; 1370.08, Use of Voice Telecommunications Services; 2710.03, Anti-Harassment Program; 1370.06, Communicating on Social Media Sites; and 2400.01, Hatch Act.

F. Use of Personal Accounts

1. Personal email is allowable for use in FDIC business if authorized or in the event of an emergency. Non-FDIC accounts are prohibited from conducting FDIC business, except when specifically required by officially provided FDIC instruction. Examples include:

   a. Password reset tools requiring personal account information;

   b. Emergency notification systems; and

   c. Business-related tasking that would otherwise identify location and timing of bank closures.

2. If a work-related email or other communication is sent or received inadvertently on a non-FDIC email account, that communication must be forwarded to an FDIC email account as soon as possible (no later than 20 days) in accordance with the FDIC Records Retention Schedule and FDIC Directives 1210.01, Records and Information Management Program, and 1360.12, Reporting Information Security Incidents (if applicable).

3. Limited Personal Use

   FDIC IT resources are intended for the accomplishment of the FDIC's mission. Personal use is permitted only when it:

   a. Does not serve as the authorized user's primary means of personal communication or IT hardware;

   b. Is limited in duration;

c. Does not adversely affect job performance;

d. Does not disrupt the work of others;

e. Does not interfere with the mission or operations of the FDIC;

f. Causes the FDIC negligible additional expense (e.g., minimal paper, ink, electricity, and data storage costs);

g. Avoids high bandwidth consumption and high cellular data usage;

h. Complies with all applicable FDIC policies and user agreements, including FDIC Directive 2710.03, Anti-Harassment Program;

i. Is conducted in accordance with the FDIC's standards of ethical conduct; and

j. Complies with prohibited use guidelines (see Prohibited Uses).

G. Prohibited Uses

The use of FDIC IT resources is prohibited for the following activities:

1. Performing any activity that is illegal under local, state, federal, or international law;

2. Engaging in political activities that violate the Hatch Act, as described in FDIC Directive 2400.01, Hatch Act;

3. Attempting to tamper with or circumvent implemented information security controls and countermeasures;

4. Operating a non-FDIC business or engaging in any other activities that violate federal or FDIC ethics regulations as described in FDIC Directive 2410.06, Standards of Ethical Conduct for Employees;

5. Communicating in a manner that violates FDIC Directive 2710.03, Anti-Harassment Program;

6. Accessing, using, displaying, storing, or transmitting pornographic, sexually explicit, sexually oriented, violent, obscene, or indecent images, files, or language;

7. Violating copyright, trademark, patent, trade secret, or licensing protections, including installing, running, or distributing unlicensed software or files;

8. Installing or using unauthorized software or services designed to share data, files, or otherwise enable direct data sharing with other users, especially those outside the FDIC;

9. Interfering with information 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;

10. Sending electronic messages to conduct official FDIC business. Electronic messages must be limited to logistical or administrative communications. In the event that an electronic message includes a decision or action of the FDIC that has not been documented elsewhere, authorized users are required to transfer the content of the message to a recordkeeping system;

11. Sending electronic messaging when driving a vehicle, while on official Government business, in accordance with FDIC Directive 1370.09, Assignments, Usage, and Safeguards of Mobile Devices; and

12. Communicating via social media sites on- or off-duty for official FDIC work or personal purposes not in compliance with FDIC Directive 1370.06, Communicating on Social Media Sites.

H. Disclaimers

All authorized users must recognize their FDIC email address associates them with the FDIC and limit participation in electronic forums (e.g., discussion groups, listservs, or news groups, etc.) in accordance with FDIC Directive 1370.06, Communicating on Social Media Sites. Those who participate in forums, or send emails containing personal opinions, may have their comments mistaken as FDIC policy. Consequently, authorized users should make appropriate disclaimers to avoid any such mistake.

I. Access to Personal Data Saved on FDIC IT Resources

FDIC IT resources should not be used to save personal data, documents, photos, or videos that are unrelated to FDIC employment. Employees have no ownership rights or guarantee to future access to such personal data they chose to save within the FDIC's IT system or on FDIC-issued devices.

J. Monitoring

1. FDIC IT resources are monitored by the FDIC. 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 any administrative, civil, or criminal action or proceeding purposes.

2. Pursuant to Section 6(a) of the Inspector General Act of 1978, the OIG may access all records.

All non-OIG requests for access of a specific authorized user's electronic information regarding any potential administrative or adverse personnel action must be approved by the following:

a. Assistant Director, Labor and Employee Relations Section (LERS), Division of Administration (DOA);

b. Assistant General Counsel, Labor, Employment, and Administration Section (LEAS), Legal Division; and

c. Chief Information Security Officer (CISO) or Deputy Director, Office of the Chief Information Security Officer (or designee).

3. Requests to search electronic information of OIG employees must be approved by the General Counsel to the Inspector General. For requests to search electronic information of employees outside of OIG (including searches for discovery purposes for administrative or court litigation, Freedom of Information Act (FOIA) requests, and Congressional requests) must be approved by the following: either the Deputy General Counsel, Corporate Operations Branch, Legal Division or the Assistant General Counsel, LEAS; and CISO (or designee).

4. 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.

5. The FDIC does not intend to monitor the content of electronic communications relating to Union activities. Should communication related to Union activities be revealed without a legitimate business purpose, it is treated as confidential.

K. Privacy

Employees should have no expectation of personal privacy with regard to the use of FDIC IT resources.

L. Disciplinary Action

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

2. Access to or use of FDIC IT resources without authorization or contrary to the law may be subject to criminal prosecution. Records produced through system monitoring and

recording in cases involving improper use of an IT resource may be used as evidence for disciplinary action and may be provided to law enforcement officials.

RESPONSIBILITIES

A. Chief Information Officer:

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

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

3. Ensures the effective use of FDIC IT resources;

4. Provides encryption capabilities to secure FDIC information; and

5. Establishes and implements FDIC IT Rules of Behavior.

B. Chief Information Security Officer:

1. Oversees the maintenance of this policy and associated Rules of Behavior for authorized users;

2. Develops and maintains FDIC mandatory Cybersecurity and Privacy Awareness training in accordance with FDIC Directive 1360.16, Mandatory Cybersecurity and Privacy Awareness Training; and

3. Approves requests for access of specific (non-OIG) authorized users of electronic information regarding any potential administrative or adverse personnel action.

C. Director, Division of Information Technology:

Issues and tracks all removable media devices that are approved (under the provisions contained in this Directive) for downloading information from an FDIC IT resource.

D. Deputy Director, Labor and Employee Relations Section:

Reviews requests for searches for electronic information that would reveal communications of a specific authorized user when needed for personnel investigations and provides approval, if appropriate.

E. General Counsel, Legal Division:

1. Reviews, or designates review of, requests to search authorized users for discovery purposes for administrative or court litigation, FOIA, and Congressional requests and provides approval, if appropriate; and

2. Reviews, or designates review of, requests in coordination with the Assistant Director, LERS and CISO for searches of electronic information that reveal specific authorized user communications and provides approval, if appropriate.

F. Supervisors/Managers:

1. Ensure authorized users under their control properly review and acknowledge the acceptable use guidelines, taking action if notified of violations to the Rules of Behavior; and

2. Request approval from LERS and the Legal Division when seeking to obtain electronic communications for a specific authorized user.

G. Authorized Users:

1. Protect the information security of FDIC-issued devices and Corporate data;

2. Report all information security breaches to supervisors/managers and the DIT Service Desk, in accordance with FDIC Directive 1360.12, Reporting Information Security Incidents;

3. Complete all mandatory cybersecurity and privacy training annually, after completing initial training; and

4. Acknowledge compliance with this Directive and associated Rules of Behavior through FDIC's mandatory Cybersecurity Awareness Training and FDIC Directive 1360.16, Mandatory Cybersecurity and Privacy Awareness Training.

H. Contracting Officers and Oversight Managers:

1. Ensure that contractors and subcontractors with network access under their management properly review and acknowledge the acceptable use guidelines, taking action if notified that their contractors have violated the Rules of Behavior; and

2. Identify contractor and subcontractor personnel without FDIC network access and who have access to sensitive information, ensuring they have taken, and continue to take, required training on an annual basis.

APPENDIX

External Authorities:

- Executive Order 13513, Federal Leadership on Reducing Text Messaging while Driving, dated October 1, 2009
- Title 5, Code of Federal Regulations, Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

FDIC Authorities:

- FDIC Directive 1210.01, Records and Information Management Program
- FDIC Directive 1360.09, Protecting Information
- FDIC Directive 1360.12, Reporting Information Security Incidents
- FDIC Directive 1360.16, Mandatory Cybersecurity and Privacy Awareness Training
- FDIC Directive 1370.06, Communicating on Social Media Sites
- FDIC Directive 1370.08, Use of Voice Telecommunications Services
- FDIC Directive 1370.09, Assignments, Usage, and Safeguards of Mobile Devices
- FDIC Directive 2121.01, FDIC Telework Program
- FDIC Directive 2400.01, Hatch Act
- FDIC Directive 2410.06, Standards of Ethical Conduct for Employees
- FDIC Directive 2710.03, Anti-Harassment Program
- FDIC Directive 2750.01, Disciplinary and Adverse Actions
- FDIC Directive 12000.01, Cooperation with the Office of Inspector General

GLOSSARY OF TERMS

Authorized Equipment: Equipment authorized for official FDIC use.

Authorized Users: Employees, contractor personnel, and any other lawful individuals who use FDIC IT resources.

Electronic Messaging: A facility for exchanging messages in real-time with other people over the Internet and tracking the progress of a given conversation.

FDIC Facility: A building, or any part thereof, including parking areas owned or leased by the FDIC.

Hands Free Device: An attachment, add-on, built-in feature or addition to a mobile device that, when used, allows the driver to maintain use of their hands.

IT Resources: Any FDIC-furnished IT equipment or IT service. Includes:

- Hardware (e.g., desktop or laptop computers, telephones, and storage devices);
- Mobile devices (e.g., tablet computers, cameras, and cellular telephones);
- Office equipment (e.g., printers, fax machines, scanners, and copiers or eCopy units); and
- Software, applications, and outsourced information services.

Jailbreaking (Rooting): The removal of software restrictions imposed by an operating system or other security mechanism.

Mobile Hotspot: A small personal device that creates a small area of Wi-Fi coverage allowing nearby Wi-Fi devices to connect to the Internet.

Peripherals: Any product that can be attached to, added within, or networked with personal computers or servers, including (but not limited to): storage, printers, scanners, monitors, keyboards, projectors, uninterruptible power supplies, and accessories.

Remote Access Systems: Options include:

- A secure, web-based remote access solution intended for use with personally owned computers using Windows.
- This solution provides access to user data (e.g., shared drives, FDICNet, and web applications) and desktop applications (including e-mail and Microsoft Office).

- A secure, web-based remote access solution intended for use with non-FDIC hardware.

- This is intended to provide mobile users basic access to FDIC computing resources without having to install specialized software on a remote computer. This solution provides access to Outlook Web Access "OWA," WebTA, and the FDICnet Homepage. Terminal Session (Remote Desktop) capability is an available option for users of this service.

- A Virtual Private Network (VPN) secure remote access system intended to provide full network access to FDIC laptops. A VPN is a network that can provide remote offices or individual users with secure access to an organization's network via the Internet.

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

Virtual Desktop Interface: Virtual Machines that reside in the cloud and allow users to connect using Remote Desktop Protocol.

Wi-Fi: Wireless technology used to connect computers, tablets, smartphones, and other devices to the internet. Wireless local area network that observes the Institute of Electrical and Electronics Engineers (IEEE) 802.11 protocol.

GLOSSARY OF ACRONYMS

CIO: Chief Information Officer

CIOO: Chief Information Officer Organization

CISO: Chief Information Security Officer

DIT: Division of Information Technology

FOIA: Freedom of Information Act

LEAS: Labor, Employment, and Administration Section

LERS: Labor and Employee Relations Section

VPN: Virtual Private Network