September 2020

The Research Foundation for The State University of New York **Acceptable Use and Security of RF Data and Information Technology**

Table of Contents

Statement of Policy

To fulfill the mission of The Research Foundation for SUNY ("RF"), it is essential that authorized users have access to RF data ("RF Data") and information technology resources ("RF Resources"). To maintain the privilege of using these assets, the RF community and other Authorized Users must follow the standards outlined in this policy. These standards require users to agree that:

- RF Resources and RF Data will be used in a responsible manner.
- They will abide by all relevant:
    - Policies and procedures, including those related to harassment, plagiarism, commercial use, theft, security, and unethical conduct, and
    - Sponsor, federal, state and local laws governing copyright and licensing infringement, unlawful intrusions, and data privacy.

Who is Covered?

This policy applies to individuals when they use RF Resources and/or are accessing RF Data.

Authorized Users and Acceptable Use

RF Resources and RF Data may only be used by authorized individuals to accomplish tasks related to their jobs. Use of RF Resources and RF Data for personal gain or to commit fraud is prohibited.

RF Data classified as confidential must be protected, and must not be disclosed without authorization. Unauthorized access, manipulation, or disclosure of confidential RF Data constitutes a security breach and may be grounds for disciplinary action up to and including termination of employment. (See the section on Security and Protecting RF Data)

User's Responsibilities

Users are responsible for:

- Reviewing, understanding, and complying with all policies, procedures and laws related to access, acceptable use, and security of RF Resources and RF Data;
- Asking Data Custodians or other officials for clarification on access and acceptable use issues not specifically addressed in RF, SUNY, or local campus policies, rules, standards, guidelines, and procedures; and
- Reporting possible policy violations to the appropriate entities listed at the end of this document.

Liability for Personal Communications and Data

Users of RF Resources are responsible for the content of their communications. The RF accepts no responsibility or liability for any Personal use of RF Resources by users. Those communicating on behalf of the RF at campus or other locations are required to follow

campus standards for communication and use of resources for these types of communications and be aware of rules regarding privacy of these communications. Any Personal data stored on RF Resources is not private, nor is the RF responsible or liable for any loss or issues resulting from the RF Data.

Privacy of Use

Users should be aware that, although the RF takes reasonable security measures to protect the security of RF Resources and accounts assigned to individuals, the RF does not guarantee absolute security and privacy. Users should also be aware of their campus policies on privacy of communications and technology use.

The RF treats the contents of individually assigned accounts and personal communications as confidential. However, the RF may examine or disclose those contents in certain circumstances, including but not limited to:

- System maintenance including security measures;
- When there exists a reason to believe an individual is violating the law or RF policy; and/or
- When required or permitted by applicable policy or law, including the NYS Freedom of Information Law.

The RF may also monitor, intercept, or access incoming, outgoing, and stored emails, text messages, instant messages, and other modes of electronic communication, as well as documents created, stored, or accessed on RF Resources. The RF also reserves the right to inspect a user's computer and other equipment used in the course of business, including but not limited to, network drives and attached electronic media.

Security and Protecting RF Data

Users of RF Data must be familiar with and follow local IT policies governing data security and technology. In the absence of local guidance users must:

- Not share computer logon and password or personal information with anyone, including supervisors, immediate colleagues, or administrative support staff;
- Not sign on with their account to grant others access to privileged resources;
- Not use someone else's ID and/or password; and
- Change temporary passwords assigned by an administrator.

Due to the level of risk that unauthorized access to, or loss of, RF Data poses to the RF and SUNY, Users should take all reasonable precautions to mitigate the risk of such unauthorized access or loss, which may include but not be limited to:

- Store work-related data to a network drive to be backed up. Doing otherwise introduces a risk of permanent data loss;
- Lock computer screens when away from the computer;
- Routinely review files and purge records no longer needed or required to be maintained by applicable record retention laws and/or policies (See the Records Management Policy);
- Avoid using simple, obvious or predictable passwords by using a combination of alphanumeric characters and/or sentences; and
- Avoid writing down passwords.

In all cases if an electronic breach occurs, you must report the incident in accordance with the RF's Notification Procedure for Electronic Breach of Information Security.

Confidential Information

Practices for Handling Confidential Information

If your job-related duties require access to Confidential Information, you must take extra precautions to protect the data, in addition to the items listed above. This can include but not be limited to:

- Do not leave sensitive documents in plain view on your desk, computer or on fax machines or copiers.
- Store sensitive documents in locked drawers or file cabinets.
- Do not release or disclose RF Data other than what is required to perform your job-related duties and in accordance with applicable RF policies and procedures on releasing or disclosing Confidential Information. (Refer to the RF's Confidentiality of Employee Information Policy and the RF's Confidentiality of Health Information Policy.)
- Ensure appropriate steps are taken when allowing consultants or third parties access to this data for work related purposes which may include but not be limited to:
  - Confidentiality Agreements
  - Receiving approval from the Data Custodian or designee.
  - Ensuring access is removed or data is destroyed or returned after the individual no longer has a need
- Use simulated data for training purposes when possible
- Strive to ensure access to RF Data follows the Principle of Least Privilege when saving data to networks
- Do not discard any Confidential Information in a waste receptacle or recycling bin (if applicable)
- Encrypt data transmissions

Mobile and Remote Access

Users Accessing RF Resources via personally owned or RF/SUNY provided devices (laptops, computers, tablets, flash drives, smart phones or other mobile devices) must take further steps to protect and ensure a secure environment including but not limited to:

- Enable a password protection/screen lock and establish automatic security timeout or auto lock after no more than 15 minutes of inactivity;
- When available, enable the application or feature so that lost or stolen devices can be traced and remotely wiped or cleared;
- Follow the standards outlined in this policy when using the device to access any RF Resource or RF Data;
- Make the device available, at the request of the RF, for the purposes of allowing the RF or its designee to review and/or extract work-related information on the device in the event of legal action or investigation.

Reporting a Suspected Violation(s)

RF employees and those acting on behalf of the RF must report a suspected violation(s) of this policy to the appropriate person (supervisor/manager, RF operations manager/designee, or department vice president) at their campus location. If the suspected violation involves an "electronic" breach of information, the operations manager/designee or department vice president must be notified per the RF's Notification Procedure for Electronic Breach of Information Security.

All reports will be held in strict confidence and promptly investigated by the appropriate person at the campus location.

Disciplinary Action Regarding a Knowing Violation

For an RF employee, disciplinary action, up to and including termination, may occur if it is determined that a knowing violation(s) of this policy has occurred. If a violation involves a SUNY employee, the RF operations manager/designee at the campus location will work with the campus SUNY official to determine the appropriate action to be taken.

Access privileges to the RF's Resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of the RF's computers and networks or to protect the RF from liability, the RF may temporarily deny access to those resources. Alleged policy violations will be referred to

appropriate RF investigative units. The RF may also refer suspected violations of law to appropriate law enforcement agencies. Depending on the nature and severity of the offense, policy violations may result in loss of access privileges, RF disciplinary action, and/or criminal prosecution.

Non-Retaliation Policy

The RF will not tolerate retaliation toward or harassment of employees who in good faith report a suspected or knowing violation(s) of this policy. The identity of individuals providing information about a suspected violation(s) will be protected within legal limits. Individuals who take retaliatory action will be subject to disciplinary action, up to and including termination.

Definitions

Authorized User

Any individual granted access to RF systems via the normal protocols in place at the campus or RF.

Least Privilege

The principle of providing a user with the least amount of access as is essential to enable that user to conduct his or her work.

RF Resources

Any network, database, computer, software applications, mobile device, flash drive, or websites provided or managed by the Research Foundation.

RF Data

Any information that relates to the operations, financial condition, employees, patents, licenses, or research of the Research Foundation, in any format, whether verbal, electronic or hard copy.

Data Custodian

The person responsible for a particular set of RF Data. This could be the PI for a project, OM or designee for campus data or central office function owner for business area specific data.

Personal Use

Any use or communications utilizing RF Resources regarding non-work related matters or other items of a personal nature.

Confidential Information

Confidential Information is defined as any RF Data that specifically identifies or describes an employee, an employee's protected health information, or RF organizational information, which if disclosed or released, a reasonable person would conclude that negative financial, competitive, or productive loss may occur and/or may cause legal or other non-beneficial impacts on the RF. It also includes information regarding any proprietary or licensed technology.

Confidential information does not include grant and contract proposal information released to sponsors and project partners as part of a formal submission, and subsequent award information and correspondence received from or sent to those parties.

Examples of Confidential Information

Additional specific examples of "confidential information" include, but are not limited to, the following items.

- an employee's name, birth date, race, gender, marital status, disability status, veteran status, citizenship, Social Security number (SSN);
- an employee's home address, home telephone number(s), relatives names, addresses, and telephone numbers;
- an employee's Personnel File;
- an employee's employment status, including leave of absence information, appointment begin and end dates, termination date, termination reason;
- an employee's payroll information, including salary rates, tax information, withholdings, direct deposit information;
- an employee's benefit enrollment information;
- an employee's Protected Health Information (PHI);
- organizational finance information, including rates and investments;
- organizational operating plans, including strategic, business, and marketing plans;
- facilities management documentation, including security system information;
- auditing information, including internal audit reports and investigative records; and

- all organizational legal documents, including pending lawsuits and attorney-client communications.

Individuals who are uncertain if the type of information being used is confidential should seek clarification from their manager/supervisor.

Contact Information – Consider Your Actions and Ask for Guidance

Where to Go for Help

If you have questions, you can seek guidance from any of the following:

- Your supervisor
- Your campus RF human resources office
- Your campus information security office
- Your operations manager or deputy operations manager
- RF Office of Compliance Services which serves as the RF's Information Security Office