SUNY RF
The Research Foundation for
The State University of New York

USER SECURITY POLICY

Table of Contents

1.0 General Terms

This document establishes a policy for The Research Foundation of State University of New York ("RF"), a private, non-profit educational corporation for maintaining a computer environment for central office and central office directed campus support operations that is controlled, consistent, and protected. This User Security Policy is designed to protect the RF data, applications, networks, and computer systems from unauthorized access, alteration, destruction, or use. Information security policies are in place for all RF users; however, please keep in mind the following:

- Given the decentralized organization structure of the RF, this policy regulates the use of technology owned and utilized at, or remotely accessed through, the central office with its principal offices located at 35 State Street, Albany, New York.
- Campus locations that share technology environments with State University of New York ("SUNY") operations must follow the SUNY Security Guidelines, as well as campus level SUNY policies in addition to any RF policies that may apply, including the User Security Policy. To the extent that security policies conflict, users should seek advice from central office RF Information Services team (contact information can be found in section 4.1 Contacts of this document). Some terminology used in this document such as job titles, departmental names, network drive names, sanctioned software etc., are specific to central office. Campus terminology may differ but the intent of the policy is still applicable.

Every user plays a critical role in ensuring the security of RF information and data. By taking the precautionary measures outlined in this document, you can reduce the risk of unauthorized access to or use of RF data, protect against identity theft, prevent unintentional security breaches, and prevent the spread of computer viruses. There are additional guidelines in Appendix A of this document that are intended to provide further information on such topics as password selection.

By using RF computer services, technology and equipment including but not limited to cellular (cell) phones, Blackberry's, pagers, laptops and data, you acknowledge that you have read, understand, and agree to adhere to our guidelines in this policy and consent to the terms described herein. Furthermore, you acknowledge that use of these services is not private and that the RF reserves the right to monitor traffic, usage patterns and any other related data. 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 systems. 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.

1.1 Definitions

The following terms are used throughout this policy.

Authorized User	An individual who is granted permission in accordance with RF procedures to access RF information and/or systems.
Blog	A Web site that allows individuals to read, write or edit.

C Drive	Where computer data is stored on your PC that is not on the network.
Central Office	RF principal offices located at 35 State Street, Albany, New York.
Chat room	A hosted Web site where a number of users can communicate in real time.
Digital Data	Data on an electronic device.
E-mail System	A specified software platform allowing for electronic communication between and amongst users and other persons, not inclusive of text and instant messaging. E-mail can be sent and received from a number of hardware platforms including but not limited to a PC, cellular telephone, and Blackberry.
Electronic Communication	Electronic messages sent from one person to another via electronic communication systems such as electronic mail ("e-mail"), text message, or Instant Messenger.
Electronic Media	Any storage device that holds digital data.
Electronic Resources	Information products that are provided through a computer or other electronic device (e.g. email, network files, online data etc.).
Encryption	A security method used to transform data from its original form into a different form to prevent unauthorized viewing or access by an individual(s) other than the intended recipient.
External or Removable Electronic Media	Any electronic storage device that holds digital data which can either be physically removed from a network or PC or can be temporarily connected to a network or PC for the purposes of transferring and storing data. The following are examples of external or removable electronic media: Hard drives, removable drives (i.e. "Zip drives"), CD-ROM, DVDs, flash memory, USB drives and floppy disks.
Health Insurance Portability and Accountability Act ("HIPAA")	Federal law designed to improve the efficiency and effectiveness of the healthcare system by standardizing the electronic data for specified administrative and financial transactions, while protecting the security and confidentiality of that information.
ID	Also referred to as "logon", "signon" "user name" or "userID". A unique combination of characters and/or numbers used to identify a specific user in a multi-user environment. The ID is usually used in conjunction with a password to gain access to RF information or systems.
Instant Messaging ("IM")	A form of text communication in real time.
Internet	Global system of interconnected computers and computer networks.

Listserv	An electronic mailing list.
Network	A system of lines and channels that are primarily designed to support individual work stations (i.e. "PCs") which users interface with via various departmental drives, i.e. the "R Drive" and the RF Web site.
Others	Any individual or user as identified above other than oneself.
Password	A unique combination of characters and/or numbers known only to the user that serves as authentication of a user's identity. The password is usually used in conjunction with a user ID to gain access to RF information or systems.
PC	A hardware device used to access the RF network including but not limited to a desktop, laptop, or tablet computer and, for the purposes of this policy, any portable electronic hardware device like a Blackberry which can be used to access the RF network.
Personal Health Information ("PHI")	Any information in a medical record that can be used to identify an individual.
Personal Information	Information related to an individual's private life or concerns in a form that permits identification of the individual. Examples of personal information can include: name, address, telephone number, race, bank account numbers, or social security numbers.
Personal Mobile Device ("PMD")	A PMD is a travel-sized computing device, typically having a display screen with touch input and/or a miniature keyboard. Examples include but are not limited to: Blackberry's, iPhone's, iPad, Droid, etc.
Personal Mobile Device Agreement	The agreement, between the RF and a PMD owner, that grants the PMD owner access to RF systems through the PMD and outlines the responsibilities and obligations that the owner will have as a result of entering into the agreement.
Remote Access	The ability to obtain access to an IT resource or the RF network from a location other than the physical building of the RF located at 35 State Street, Albany, New York.
Social Networking Site	A hosted site where online groups of people share interests and interconnect which may display personal information, e.g. Facebook, MySpace, and LinkedIn.
Systems	One or more computers and associated software (i.e. programs used to operate computers) that make up the RF network.
User	Any individual including, but not limited to an RF employee, non-employee, associate, or independent contractor and any other individual or entity, i.e.

	corporation, partnership, Limited Liability Company ("LLC"), internal entities or affiliate corporations and other software entities with access to RF electronic media or electronic data.
Vendor	Any individual or company from whom the RF has purchased or entered into an agreement for goods or services.

1.2 Purpose

The purpose of the user security policy is to:

- Communicate to users their responsibilities for RF information technology and related equipment to ensure the computing environment is safeguarded and prevent compromise of confidential, mission-critical data;
- Establish understanding in the user community as to the distinction between acceptable and unacceptable use of computing resource;
- Allow compliance with applicable internal and external controls, regulations and policies;
- Provide a means for internal and external security related inquires or issues; and
- Establish security procedures that help protect the reputation of the RF with external parties including SUNY, sponsors, vendors, government officials and the general public.

1.3 Scope

This security policy pertains to users of RF computer services, technology, equipment and data.

2.0 Acceptable and Unacceptable Use

This policy is a guide to the acceptable use of RF computer services, technology, equipment (e.g. including but not limited to, cell phones, Blackberry's, pagers, laptops, tablet PCs) and data. Other RF policies/procedures may impact acceptable or unacceptable use. Each individual is responsible for ensuring the protection and proper use of the software, equipment and data in their care.

Unacceptable and prohibited general activities include, but are not limited to, the following:

- Revealing your username and password to others, or signing on with your account to grant others access to your privileged resources;
- Using someone else's ID and/or password;
- Using RF systems for personal commercial purposes or personal monetary gain (e.g. personal blog hosting, Web hosting);
- Using the RF network as a means to gain unauthorized access to non-RF systems/networks or to allow non-RF authorized users to gain unauthorized access to RF systems/networks;
- Using your authorized access to RF systems or information for unlawful or otherwise inappropriate reasons;

- Using illegal or unlicensed software, including but not limited to, file sharing services such as LimeWire or BitTorrent;
- Copying and/or distributing commercial software without proper licensing;
- Knowingly creating, executing, forwarding, or launching any harmful computer code;
- Downloading and storing personal data on network drives is prohibited;
- Using the C drive for anything other than storing personal data including, but not limited to, legally obtained personal music collections and other work-place appropriate personal documents;
    - Questions regarding whether or not personal data is acceptable in the workplace may be directed to the Office of Human Resources; and
    - The user's respective departmental vice president or assistant vice president or RF Information Services can disallow this privilege at any time due to abuse.

2.1 Internet Use

The RF provides and maintains access to the Internet for purposes of supporting its fundamental activities.

Users are expected to follow the necessary safety measures outlined below. Internet use policies and prohibited activities include, but are not limited to, the following:

2.1.1 Acceptable Use of the Internet

Access to the Internet is provided for the conduct of official business.

2.1.2 Unacceptable Use of the Internet

The following are unacceptable uses of the Internet:

- Use for any personal monetary interests or gains,
- Activities which are obscene or otherwise violate any federal, state, or local law or ordinance or RF policies, procedures, or guidelines,
- Activities that could create potential civil liability, such as libel or slander,
- Activities that departmental or corporate management defines as disruptive to the workplace or unethical or unprofessional based on observation or awareness of activity,
- Communication with media or the public by anyone not designated and expressly authorized to speak on behalf of the RF through technological forums (e.g. blogs, social networking sites, news groups, listservs, instant messaging, and chat room).
    - The RF is not responsible for non-RF sponsored business use of such forums and the RF disclaims original liability for the use of such forums other than in the scope of user's employment with RF;
- Intentionally disabling, impairing, or overloading performance of any RF or Internet systems or applications.
- Bypassing security on any workstation or system to gain access to a restricted service or compromise the privacy of another user (i.e. hacking)

- Transmittal of RF material (e.g. copyrighted software, internal correspondence, etc.) to any computer, Web site or other external electronic media without prior permission from Information Services.

2.1.3 Internet Use Principles and Standards

The following are general principles and standards for Internet use:

- The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. When such transfer is required, appropriate steps must be taken to minimize risk. Information Services must be contacted for assistance;
- Transmitting personal information, confidential information or protected health information ("PHI") over the Internet must comply with applicable requirements of state and federal regulations (e.g. HIPAA). Information Services must be contacted for approval;
- Personal use of the Internet is a privilege, not a right. Personal use of the Internet should not impede the conduct of RF business and must follow this policy and other related policies set forth by the Office of Human Resources, Information Services and departmental vice presidents. The user's respective departmental vice president or assistant vice president or Information Security can disallow this privilege at any time due to abuse; and
- The RF disclaims any liability related to the personal use of the Internet and does not guarantee the integrity of any non-business related data or usage.

2.2 Electronic Communications

Electronic Communications security is a joint responsibility of RF Information Services staff and e-mail users. Users must use their best effort to secure RF data and electronic resources. Attached files received from outside the local area network will automatically be scanned with virus detection software. This software will not necessarily detect all viruses. Suspicious activity should be immediately reported to Information Services.

2.2.1 Acceptable Use of Electronic Communications

The following are acceptable uses of electronic communications:

- Use in support of RF business, however:
    - Users may use electronic communications to communicate informally with others so long as the communication does not violate professional standards of conduct; and
    - E-mail is intended for outside communications as related to legitimate business activities within job assignments or responsibilities. As with any other communication medium, employees are expected to conduct themselves professionally, and to comply with the Office of Human Resources policies on communications and work environment as stated above. Limited use for non-work related purposes is anticipated; however the same use policies apply.

The user's respective departmental vice president, assistant vice president or Information Security can disallow this privilege at any time due to abuse.

2.2.2 Unacceptable Use of Electronic Communications

The following are unacceptable uses of electronic communications:

- Any use that would jeopardize the legitimate interest of the RF such as, but not limited to:
    - personal gain or for any personal monetary interests or gains;
    - any activities which are obscene or otherwise violate any federal, state, or local law or ordinance or RF policies, procedures, or guidelines;
    - any activities that could create potential civil liability, such as libel or slander, and/or
    - any other activities which Management feels are disruptive to the workplace are unethical or unprofessional.
- Transmitting personal information, confidential information or PHI through e-mail that does not comply with applicable requirements as defined in federal and state law or RF policies, procedures, or guidelines. Information Services must be contacted for approval.

2.2.3 Electronic Communication Use Principles and Standards

The following are general principles and standards for electronic communications:

- E-mail messages are not considered personal or private, are stored electronically even after deletion from the user mailbox and can be monitored or retrieved at any time by the RF;
- All e-mail messages may be subject to discovery proceedings in legal actions.
- E-mail shall be retained and deleted in accordance with applicable RF electronic message retention and destruction policies;
- Consider the organizational impact before sending, filing, or destroying e-mail messages;
- Follow the mandates of the Office of General Counsel and Secretary on e-mail preservation in legal proceedings; and
- Follow the RF User Security Policy and other RF policies on personal and professional conduct and ethics.

3.0 Security Controls

The following section pertains to RF logical and physical security controls. There are user guidelines in Appendix A that provide assistance to users on how to protect data.

3.1 Logical Security

System access is centrally governed and administered for centralized campuses and central office. At central office, the point of contact is Customer Services. Users only gain access to the RF network and computer systems with proper approval from the individual's manager and with guidance from Information Services staff.

- Access is based upon job duties and requirements/needs in the individual's job description. System access is confirmed on an annual basis by Information Services.
- Requests for specific types of access (e.g. payroll) require additional approvals based upon the procedures in place;

- Access is governed centrally by Information Services and administered for centralized campuses and central office by Customer Services, who maintains a list of specific access procedures by area;
- Contractor or vendor system access must be approved by the responsible manager as well as Information Services; and
- System access is immediately removed upon the severance of the working relationship. Access will be modified as job duties or functions are revised. The Human Resources department provides notification to Customer Services when termination of access is required or if job duties change.

3.1.1 ID and Password

Passwords are an important control for computer security and are used for authentication to the RF network and business applications. Network passwords will be changed every sixty days and business system passwords will be changed every ninety days. Users will be prompted when passwords need to be updated, and may change passwords more frequently as needed.

The following basic criteria apply to individual password use (specifics are governed by a password policy owned by the Central Office):

- Passwords must not be shared with others;
- Each user must have a unique ID and password;
- Passwords must be changed immediately and notification given to Information Assurance if your password has been lost, stolen or shared; and
- Network Passwords must be at least five characters long. Business applications passwords must be at least eight characters, one of which must be numeric.

3.1.2 Software Acceptable Use

It is RF policy to respect all computer software copyrights and to adhere to the terms of all software licenses to which the RF is a party. RF users may not duplicate any licensed software or related documentation for use either on RF premises or elsewhere unless they are expressly authorized to do so by agreement between the licensor and the RF. Unauthorized duplication of software may subject users and/or the RF to both civil and criminal penalties under the United States Copyright Act. Users may not give licensed software to any other parties including, but not limited to, contractors and customers. RF users may use software on local area networks or on multiple machines only in accordance with applicable license agreements without further approval from the Office of General Counsel and Secretary and Information Services, however if no license agreement exist than approvals must be sought from these departments.

- To purchase software, users must contact Information Services through Customer Services, to ensure the software is properly tracked and registered through the controls in place. Users are not permitted to acquire software and install it on RF computers without contacting Customer Services for appropriate review by an Information Services staff member. Documentation, user manuals, program files and other pertinent items must be retained and made available to the appropriate Information Services staff; and

- Non-supported software may be purchased by the user's office after review by the appropriate staff in Information Services. All support for the user acquired software will be the sole responsibility of the user or department purchasing the software.

3.1.3 Remote Access to RF Network and Business Applications

Remote access is managed, upon request, by Customer Services. Users only gain remote access to the RF network and computer systems with proper approval from the individual's manager and with guidance from Information Services staff. Remote access is:

- Based upon job duties and requirements/needs in the individual's job description.
- Confirmed on an annual basis by Information Services; and
- Immediately removed upon the severance of the working relationship or may be modified as job duties or functions change. The Human Resources department provides notification to Customer Services when termination of access is required or if job duties change.

Remote users must take and accept a higher level of responsibility for all RF electronic information and data accessed by them from outside the physical location of the RF. The policies below apply to any remote connection to the RF, including Outlook Web Access.

Below are rules that must be followed to ensure the protection of RF data entrusted to your care:

- By using remote access technology with non-RF owned equipment, users must understand that the machine in use is, in effect, an extension of the RF's network while connected to the RF network, and as such, is subject to the same rules and regulations that apply to RF owned equipment;
- Non-RF owned computers used to connect to the RF network must use the most up-to-date virus protection software and security patches;
- Only RF-sanctioned technologies can be used to connect to the RF remotely such as VPN or VM View. It is the responsibility of users with remote access privileges to ensure that unauthorized users are not allowed access to RF internal networks and resources;
- Remote access use to the RF network is to be controlled using user authentication and password protection;
- Passwords for remote access shall not be saved on end-user computers or devices;
- RF data should not be downloaded or saved to non-RF network or device (i.e. floppy disks, memory sticks, and other removable electronic media, or home computer). Use RF network shared drives to save information, rather than local hard disk drives or diskettes;
- It is the responsibility of the user to be aware of specific information handling requirements when working with RF data via a remote connection (i.e. applicable regulations such as HIPAA);
- Remote access for contractors, vendors, or other non-RF employed individuals must be approved by the responsible manager as well as Information Services; and
- Operating location-based RF employees visiting the central office may be provided with access to the Internet through the RF network.

3.2 Physical Security

Building access to the RF office floors is restricted and a key card is required. Access is requested and granted through the Human Resources department.

- Building access is generally provided to the floor the individual works on and must be approved by individual's vice president. Certain areas of the building are restricted and require special approval for access in addition to the individual's vice president.
    - For example: access to the data center and communications (i.e. TELCO room) requires approval from Information Services. If access for contractors is required, the responsible manager should request approval from customer services (customerservices@rfsuny.org). If approved, access will be granted for a specific period of time.

3.3 Training

This policy will be provided to new users as part of orientation. Training on the RF User Security Policy will be required for central office staff on an annual basis through the RF Learning Center.

3.4 Penalties and Reprimands

An RF central office user who fails to comply with the RF User Security Policy will be disciplined, up to and including termination, as deemed appropriate by RF Management.

4.0 Getting Help

The following section provides assistance through contact information and related resources.

4.1 Contacts

Joshua Toas
Chief Compliance Officer
rfcompliance@rfsuny.org

4.2 Related Resources

RF Confidential Information Policy

Notification Procedure for Electronic Breach of Information Security

Notification for Breach of Privacy of Protected Health Information

Ethics Hotline

Conflict of Interest Policy

4.3 Exceptions/Questions

Any exceptions, disputes or questions related to the RF User Security Policy should be brought to the attention of Information Security. Management reserves the right to make exceptions to this policy when circumstances require review due to impact on administration or usability.

Appendix A- User Guidelines

Protect Electronic Data

- Do not leave sensitive documents in plain view on your computer screen.
- Store work-related data to a network drive such as your Y: drive to ensure it is backed up. Doing otherwise introduces a risk of permanent data loss.
- Ensure that all confidential data is stored on a secured network drive where only authorized users may gain access.
- Do not store confidential data on a laptop or other mobile device as said devices can be easily stolen.
- Routinely review electronic files and purge files that are no longer needed in accordance with record retention laws and/or policies.

Protect Non Electronic Data

- Do not leave sensitive documents in plain view on your desk or on fax machines or copiers.
- Store sensitive documents in locked drawers or file cabinets.
- Shred confidential paper documents when they are no longer needed in accordance with record retention laws and/or policies.

Secure Your Computer

- Always lock your computer screen when away from your desk.
- Never give your computer logon and password or personal information to anyone.
- Avoid using simple, obvious or predictable passwords; use a combination of alphanumeric characters and/or sentences.
- Avoid writing down passwords or posting them in public view.
- Always change temporary passwords assigned by an administrator.
- Take extra precautions to secure laptops and other mobile devices when away from your desk or traveling.

Exercise Caution

- Do not open e-mail attachments from an unknown source or an attachment you weren't expecting, even if it appears to be coming from someone you know.
- Do not visit unknown Internet sites.
- Do not download or install software without approval; requests should be submitted through Customer Services. All software installs are tracked and recorded.
- Do not reply to or forward spam or junk e-mail (i.e. unsolicited e-mail) unless otherwise directed by Information Services support staff.
- Avoid sending personal or confidential information in an e-mail whenever possible and, if essential, necessary pre-cautions should be taken such as adding a confidentiality statement to the e-mail message.

- Do not provide information over the phone without knowing if the person on the other end is authorized to receive it and without being certain of their identity.
- Maintain a constant awareness about information and data in any format; preventing unauthorized personnel from seeing or overhearing confidential or private information.
- Report suspicious activity to your supervisor and/or directly to a member of the Information Security group.

Change Record

Date	Author	Version*	Description of Change*
5/7/2010	Carpenter	1.0	• Initial document
4/26/2011	Kowalski	1.1	• Changes for Organization changes and clarity.
9/5/2011	Bartoletti	1.2	• General grammar and formatting updates and section about personal mobile devices section 4
9/12/2011	Bartoletti / Toas	1.3	• Edited section about PMD and added a definition for them
11/8/2011	Bartoletti/Agnello	1.4	• Final version based on edits for PMD and others
11/21/2011	Bartoletti	1.5	• Final version for review with CISO
3/23/2012	Bartoletti	1.6	• Backed out the PMD changes, updated the logo, and sent for reposting as the document for FY12 (no changes for FY12 were completed for PMD so they will be updated later (see changes 1.2 through 1.5 and latest version of document for those changes incorporated)
11/29/12	Sidarous	1.7	• Edited contact information to Joshua Toas
05/17/13	Sidarous	1.8	• Updated link