RF Confidential Information Policy

Effective Date:	October 21, 2021
Supersedes:	RF Confidential Information Policy dated September 14, 2007
Policy Review Date:	To be Reviewed every 3 years from effective date
Issuing Authority:	Research Foundation President
Policy Owner:	Chief Compliance Officer
Contact Information:	(518) 434-7145 RFCompliance@rfsuny.org

Reason for Policy

The RF maintains a significant amount of Confidential, proprietary, and personal Information. This Information is a professional resource for RF employees enabling the RF to efficiently carry out its business; however, the data is a potential target of cyber criminals, hackers, and others who could utilize it for wrongful or criminal purposes. This policy helps mitigate the growing internal and external threat to RF data and Confidential Information.

Statement of Policy

All RF employees and those acting on behalf of the RF who have access to confidential RF Information or Information of a third party that the RF is obligated to keep confidential, will ensure that this Information is treated in accordance with the "Requirements for Maintaining Confidential Information" below.

In addition, all RF employees and those acting on behalf of the RF are responsible for immediately reporting any suspected violation(s) of this policy or any other action which violates confidentiality of RF information to the manager/supervisor, department vice president/unit director, or RF Operations Manager/designee, as appropriate, at the campus location.

Requirements for Maintaining Confidential Information

All RF employees and those acting on behalf of the RF with authorized access to Confidential Information stored on the RF network, in any media or electronic format, or in hard copy, are required to protect this Information. The following rules govern access to and use of Confidential Information:

1) Unauthorized use of Confidential Information is not permitted. RF employees and those acting on behalf of the RF with authorized access to Confidential Information may only access the Confidential Information for the sole purpose of performing job-related duties.
2) Confidential Information cannot be used or accessed for personal benefit or the benefit of others.
3) Those with access to RF data or business systems will not enter, add, change, delete, disclose, exhibit or release RF owned data, including Confidential Information, unless doing so is authorized for a specific business purpose and consistent with the individual's job-related duties, and is consistent with

applicable laws, rules, and policies, including 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.)

4) Personal passwords must be protected and never disclosed to anyone, including representatives of the Department of Information Technology Services or Customer Services/Help Desk. If you suspect your password has been compromised, immediately change it and report the compromise to Customer Services.

5) RF employees and others with access to Confidential Information must:

   a) Keep Confidential Information on desktops or on computer screens from being viewed by others that do not require access.

   b) Lock computer screens when away from their desk or office.

   c) Use simulated training Information when possible; when this is not possible, make efforts to protect and/or disguise Confidential Information.

6) Confidential Information should, whenever possible, be stored on the user's personal LAN drive, in a locked office, or locked cabinet/drawer. Confidential Information that requires viewing by more than one individual will either be stored on a restricted public drive or password protected.

7) RF owned data, including Confidential Information, must be disposed of in accordance with applicable laws and/or RF policies on record retention. Individuals must not discard any Confidential Information in a trash or recycling bin without shredding the Confidential Information prior to disposal. Refer to the RF's:

   a) Records Management Policy
   b) Record Retention for Person-Related Records
   c) Record Retention for Account Expenditure Records
   d) Record Retention for Project Administration Records
   e) Record Retention for Technology Transfer Records
   f) Destruction of Records Guideline

8) RF employees must not remove Confidential Information from work premises without proper authorization. At the Research Foundation Central Office, your department vice president or unit director is authorized to provide you with necessary authorization. At a campus operating location, authorization may be obtained from your Operations Manager, Deputy Operations Manager, or functional director with delegated authority to carry out Research Foundation business.

9) Confidential Information must not be disclosed to consultants without receiving prior approval from the Operations Manager or designee at a campus operating location, or by your department vice president or unit director at the Research Foundation Central Office. Consultants may not remove Confidential Information from the local premises without prior authorization. When Confidential Information is shared with consultants, a confidentiality agreement or non-disclosure agreement is required. The agreement must include information regarding disposal and return of all RF owned data or Information.

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 their Operations Manager, Deputy Operations Manager, supervisor/manager, the RF's Office of Compliance Services, the RF's Office of General Counsel and Secretary, the RF's Office of Internal Audit Services, the Speak Up RF – Ethics Hotline, or their department vice president. If the suspected violation involves an electronic breach, 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

Violation of this policy may result in discipline pursuant to the RF's Progressive Discipline Policy, or for non-RF users, removal of any delegation of authority.

Responsibilities

The following table outlines the responsibilities for compliance with this Policy:

Responsible Party	Responsibility
All RF employees and those acting on behalf of the RF	Abide by this policy for maintaining Confidential Information. Report a suspected violation(s) of this policy to the appropriate person at the campus location or Central Office (manager/supervisor, Operations Manager/Deputy Operations Manager/designee, department vice president/unit director).
Manager/Supervisor	Abide by this policy for maintaining Confidential Information. Encourage all RF employees and those acting on behalf of the RF to abide by this policy. Report a suspected violation(s) of this policy to the appropriate person at the campus location (Operations Manager/designee) or Central Office (department vice president or unit director) to protect both the alleged violator and the individual reporting a potential violation.

	Do not retaliate against the alleged violator or the individual reporting a potential violation(s).
RF Operations Manager/Deputy Operations Manager/designee at the campus location	Abide by this policy for maintaining Confidential Information. Encourage all RF employees and those acting on behalf of the RF to abide by this policy. Authorize the removal of Confidential Information from the work premises in accordance with this policy. Authorize the disclosure of Confidential Information to consultants acting on behalf of the RF. Report a suspected violation(s) of this policy to the Vice President for Human Resources or designee at Central Office to protect both the alleged violator and the individual reporting the violation(s). Investigate a reported suspected violation(s) and determine if a violation(s) did or did not occur. Do not retaliate against the alleged violator or the individual reporting a potential violation(s). Work with the campus SUNY official if a violation occurs involving a SUNY employee. Communicate to the appropriate personnel at the campus location any disciplinary action that will occur as a result of an actual violation(s) of this policy.

Department Vice President/Unit Director at Central Office	Abide by this policy for maintaining Confidential Information. Encourage all RF employees and those acting on behalf of the RF to abide by this policy. Authorize the removal of Confidential Information from the work premises in accordance with this policy. Authorize the disclosure of Confidential Information to consultants acting on behalf of the RF. Investigate a reported suspected violation(s) and determine if a violation(s) did or did not occur. Do not retaliate against the alleged violator or the individual reporting a potential violation(s). Communicate to the appropriate personnel any disciplinary action that will occur as a result of an actual violation(s) of this policy.
Chief Compliance Officer, Central Office	Interpret sections of the policy relating to maintaining Confidential Information and guide campuses through implementation of the policy as requested. Revise policy as needed.
Vice President for Human Resources or designee, Central Office	Interpret sections of the policy relating to employee Information and guide campuses through implementation of these aspects of the policy as requested.

Definitions

Information- any communication or reception of knowledge regarding the RF and includes facts, data, or opinions that may consist of numerical, graphic, or narrative forms, whether oral, downloaded to equipment, or maintained in mediums, including, but not limited to, computerized databases, papers, microfilms, magnetic tapes, disks, CDs, flash drives, and cell phones.

Confidential Information- any RF "Information" as described above that specifically identifies and/or describes an employee, an employee's Protected Health Information, and/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 or Information that has been provided to the RF by another party for which the RF has confidentiality obligations.

Confidential Information does not include grant and contract proposal information released to sponsors and project partners as part of a formal submission, 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. Individuals who are uncertain if the type of information being used is confidential should seek clarification from their manager/supervisor.

- 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
- all organizational legal documents, including pending lawsuits and attorney-client communications
- technical information provided to the RF by a sponsor under confidentiality provision

Related Information

Notification Procedure for Electronic Breach of Information Security
Confidentiality of Employee Information Policy
Records Management Policy
Record Retention for Person-Related Records
Record Retention for Account Expenditure Records

Record Retention for Project Administration Records
Record Retention for Technology Transfer Records
Destruction of Records Guideline
Progressive Discipline Policy

Forms

None

Change History

Date	Summary of Change
January 4, 2024	Updated Ethics Hotline name and Link
June 22,2023	Removed link and reference to obsoleted Breach of Privacy of Protected Health Information Procedure and related definitions
April 7, 2022	Added links to new Technology Transfer Record Retention Schedule and Destruction of Records Guideline.
October 21, 2021	Consolidated the Requirements for Maintaining Confidential Information into nine items; put in new template format; added reference to Notification Procedure for Electronic Breach of Information Security. “Responsibilities” table re-organized to clarify campus and RFCO roles, and language added prohibiting retaliation against individuals reporting violations or accused of violations. Definition of “Confidential Information” revised.
September 14, 2007	New document.

Feedback

Was this document clear and easy to follow? Please send your feedback to webfeedback@rfsuny.org.