Notification Procedure for Electronic Breach of Information Security

Effective Date: March 18, 2022
Function: Office of Compliance Services
Contact: RFCompliance@rfsuny.org

Basis for Procedure

This document outlines the notification and response procedure that the Research Foundation ("RF") will follow if there is an actual or suspected breach of the RF's information systems. RF employees and those acting on behalf of the RF have an obligation to report any actual or suspected breach of the RF's information systems they become aware of. A breach of the RF information systems is an unauthorized acquisition or access of electronic data which compromises the security, confidentiality, or integrity of Private and Personal data.

Breaches of information security are not limited to computer hacking. An information security breach can occur if an unauthorized person gains access to Personal and Private information, such as from a stolen or misplaced laptop, tablet, smart phone, flash drive or any other electronic device capable of storing data that contains private information, or by any other unauthorized receipt of or access to Personal and Private information.

Pursuant to applicable laws and regulations, the RF is required to provide notification when information systems are breached if Personal and Private information is available to unauthorized individuals.

Procedure

If a Suspected Security Breach Occurs at Central Office

The following table outlines the steps to take when a suspected electronic security breach occurs at central office:

Step	Action
1	The person who suspects that an electronic security information breach may have occurred notifies his/her respective RF department vice president ("VP").
2	The VP notifies one of the following Information Security personnel: • Joshua Toas, Chief Compliance Officer/Chief Information Security Officer (joshua.toas@rfsuny.org) • Jason Holbrook, Deputy Information Security Officer (jason.holbrook@rfsuny.org) • Duane Mysliwiec, Associate Director of IT Operations, Infrastructure & Security (duane.mysliwiec@rfsuny.org)
3	Information Security works with appropriate technical and other personnel to analyze the situation to determine if a breach has occurred.

Step	Action
4	In the event of a suspected breach, Information Security notifies the RF President and other RF leaders as appropriate.
5	The Office of General Counsel and Secretary provides legal support as needed.
6	The Office of Compliance Services works with Information Technology Services to determine whether a breach has occurred. If so, Compliance will notify appropriate regulatory bodies (NY Attorney General, NY State Police, NY Consumer Protection Board), and if greater than 5000 NY residents are impacted, will work with Human Resources to notify impacted residents and credit reporting agencies.
7	Compliance Services facilitates filing any applicable insurance claims.
8	Compliance, in consultation with Information Technology, communicates status information with the affected person's department VP.
9	The Office of Corporate Communications develops a notification message to the affected individual(s) in consultation with the RF Leadership and determines from which office the notification will be issued.

If a Suspected Breach Occurs at a Campus

The following table outlines the steps to take when a suspected electronic security breach occurs at a campus:

Step	Action
1	Campus representative who suspects that an electronic information breach has occurred related to RF data or systems notifies the Operations Manager at the campus.
2	Operations manager notifies one of the following central office Information Security personnel: • Joshua Toas, Chief Compliance Officer/Chief Information Security Officer (joshua.toas@rfsuny.org) • Jason Holbrook, Deputy Information Security Officer (jason.holbrook@rfsuny.org) • Duane Mysliwiec, Associate Director of IT Operations, Infrastructure & Security (duane.mysliwiec@rfsuny.org)
3	Information Security works with appropriate technical and other personnel to analyze the situation to determine if a breach has occurred.
4	In the event of a suspected breach, Information Security notifies the RF President and other RF leaders as appropriate.
5	The Office of General Counsel and Secretary provides legal support as needed.
6	The Office of Compliance Services works with Information Technology Services to determine whether a breach has occurred. If so, Compliance will notify appropriate regulatory bodies (NY Attorney General, NY State Police, NY Consumer Protection Board) and if greater than 5000 NY residents are impacted will work with Human Resources to notify impacted residents and credit reporting agencies.
7	The Office of Compliance Services facilitates filing any applicable insurance claims.
8	Compliance, in consultation with Information Technology, communicates status information with the affected person's department OM.

Step	Action
9	The Office of Corporate Communications develops a notification message to the affected individual(s) in consultation with the RF Leadership and determines from which office the notification will be issued.

Definitions

Personal Information- any information that can be used to identify a specific person, such as his or her name, number, personal mark, or other identifier.

Private Information- A username or email address in combination with password or security question and answer that would permit access to an online account, or Personal Information in combination with any one or more additional piece of information from the following list:

- Social security number;
- Driver's license number or non-driver ID number;
- Account number, credit or debit card number, with or without a security code, access code, or password, or other information that would permit an unauthorized person could gain access to an individual's financial account; or
- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
- Username or email address in combination with password or security question and answer that would permit access to an online account

Related Information

Acceptable Use and Security of RF Data and Information Technology

Forms

None

Change History

Date	Summary of Change
July 23, 2024	Updated Information Security Personnel.
April 26, 2024	Updated Information Security Personnel.
June 22, 2023	Removed link to obsoleted procedure and related definition

Date	Summary of Change
May 30, 2023	Updated Information Security personnel.
May 3, 2023	Updated Information Security personnel.
May 13, 2022	Added Deputy Information Security Officer to Information Security personnel.
March 18, 2022	Revised in new procedure format; updated contact information, definitions, and procedure steps.
May 13, 2011	Replaced Christine Carpenter's contact information with Mike Bartoletti.
August 31, 2010	Updated Internal Audit and External Relations contact information.
November 2, 2009	Updated General Counsel contact from Jim Dennehey to Joshua Toas.
March 28, 2007	Deleted reference to Tim Murphy.
July 5, 2006	Reordered contacts under Step 2 in each table and changed "operating location" to campus.
March 7, 2006	New Document.

Feedback

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