
ACCEPTABLE USE OF RESEARCH FOUNDATION PROPRIETARY DATA OUTSIDE THE RF BUSINESS SYSTEM POLICY

Category: Research
Responsible Office: Sponsored Projects Services
Responsible Executive: Vice President for Research

Date Established: 12/3/08
Date Last Revised: -
Date Posted to Library: 12/17/08

Summary

The integrity and confidentiality of Research Foundation (RF) data must be protected when RF proprietary data are combined into a non-RF business system.

Policy

POLICY STATEMENT

RF proprietary data are private and confidential data that must be protected. All proprietary data extracted from the RF business system must be protected from unauthorized access. Individuals with authorized access to RF proprietary data are required to adhere to the following University at Buffalo (UB) information security policies to provide a secure environment where the privacy and confidentiality of proprietary data are protected.

New York State Information Security Policy

The NY State Information Security Policy is a comprehensive policy that sets forth the minimum requirements, responsibilities and accepted behaviors to establish and maintain a secure environment. UB has adopted the NY State Information Security Policy as its umbrella computer and information security policy.

University at Buffalo Policy on Securing Network-Connected Devices

This policy details the requirements that must be followed when devices are connected to the university network.

University at Buffalo Password Policy

This policy establishes the requirements that all UB passwords must follow.

University at Buffalo Protection of Regulated Private Data Policy

This policy outlines the university's commitment to protecting regulated private data to safeguard the privacy of the university community, reduce the threat of identity theft, and comply with state and federal laws and regulations.

University at Buffalo Standards for Securing Regulated Private Data

The security measures required to protect regulated private data are detailed in this policy.

University at Buffalo Data Access and Security Policy

This policy defines the access requirements for regulated private data and includes the roles and responsibilities for those granting access.

BACKGROUND

The Research Foundation central office has issued the *Policy on Acceptable Use of Research Foundation Data Outside of RF Business Systems*, providing campus requirements for access to and use of proprietary data the RF considers being private and confidential. In order to comply with the RF policy, a University at Buffalo campus policy is required to ensure that:

the university provides a secure environment with proper controls to protect the privacy, integrity, and confidentiality of extracted proprietary data combined in a non-RF business system

appropriate campus policies, procedures, and standards are in place to ensure that access and use of the data are consistent with a business need-to-know.

DEFINITIONS

RF Data - Corporate, agency, and sponsored program data that is classified into two types: proprietary and non-proprietary.

Proprietary Data – RF data that is private and confidential. Examples include, but are not limited to:

- Biographical data (e.g. age, sex, marital status)
- Elected benefits
- Financial sponsored program data at the detail level
- FLSA designation (exempt or non-exempt)
- Health Insurance Portability and Accountability Act (HIPAA) related data
- Home address
- Home phone
- Job title
- Salary
- Social Security Number

Non-proprietary Data – high-level data that is not considered private and confidential including financial sponsored program data at the aggregate level (no detail) and personal data limited to name, work telephone number, department/location, and employee identification number (as long as this number or its placement in a sequence of numbers does not identify the person's employer as the RF).

RESPONSIBILITY

Operations Manager (OM)

Certify that an environment with appropriate policies, procedures, and controls is in place to protect RF data.

Authorize access to RF proprietary data consistent with a business need to know.

Utilize the “Authorization for Use of Research Foundation Data outside the RF Business System” form, to annually provide the RF with a list (by name or job description) of university employees authorized to access extracted proprietary data.

In the event of a security breach or a suspected security breach, contact the RF. Follow the process outlined in the RF’s “Notification Procedure for Electronic Breach of Information Security.”

The OM or designee is authorized to provide proprietary RF data to a sponsor if the data is related to an applicable sponsored program grant or contract for which there is a contractual obligation to provide the information, or if providing the data is a requirement of obtaining a sponsored program grant or contract.

Information Security Officer

Conduct annual security reviews of approved systems storing and handling extracted proprietary RF data.

Periodic scans of workstations, servers, and network traffic, for RF data may also be implemented.

Individuals Authorized to Access Extracted RF Proprietary Data

Complete the University at Buffalo [Access to Information Compliance Form](#) before access will be granted in order to acknowledge their responsibilities to protect the extracted proprietary RF data, comply with confidentiality requirements, and comply with all UB information security and data protection policies.

APPLICABILITY

This policy applies to all university entities, any official or administrator with responsibilities for managing extracted proprietary RF data, and those employees who are entrusted with extracted proprietary RF data.

COMPLIANCE

Any employee or student who breaches this policy on confidentiality of extracted proprietary RF data will be subject to disciplinary action and/or sanctions up to and including discharge and dismissal in accordance with University policy and procedures.

Contact Information

Information Security Officer
517 Capen Hall
University at Buffalo
sec-office@buffalo.edu
(716) 645-8126

Related Information

University Documents:

[Access to Information Compliance Form](#)
[Application Service Provider IT Security and Service Criteria](#)
[Information Security: Data Access and Security Policy](#)
[Social Security Number Policy](#)
[Protection of Private Regulated Data Policy](#) – Interim Policy
[Standards for Securing Private Regulated Data](#) – Interim Policy
[Policy on Securing Network-Connected Devices](#)

Other Documents:

[New York State Information Security Policy](#)
[New York State Cyber Security Incident Reporting Procedure](#)
Acceptable Use of Research Foundation Business System Data Outside the RF Business Systems Policy
https://portal.rfsuny.org/portal/page/portal/Pers_Admin/Employee%20Relations/authorization_use_RF_data_outside_RF_business_system.pdf
RF's Notification Procedure for Electronic Breach of Information Security
https://portal.rfsuny.org/portal/page/portal/Business_applications/Security%20Administration/pro_hr_notification-breach-info-security.htm

Related Links:

[New York State Information Security Breach and Notification Act](#)
<https://www.pcisecuritystandards.org/>
[Gramm-Leach-Bliley Act](#)
[Privacy Act of 1974](#) (includes protection of Social Security Numbers)

Presidential Approval

Signed by President John B. Simpson

John B. Simpson, President

12/3/08

Date