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

Date Established: May 20, 2008
Date Last Revised: July 30, 2008
Date Posted to Library: -

Category: Information Technology
Responsible Office: CIO

Summary

The integrity and confidentiality of Research Foundation (RF) data must be protected. Data protection policies, procedures, and standards must be followed when RF proprietary data are extracted from the RF business system and 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. The University's Operations Manager (OM), the Executive Vice President for University Support Services, is responsible for the protection of RF proprietary data and authorizes access to extracted RF proprietary data based on a business need-to-know.

Individuals with authorized access to extracted RF proprietary data are required to adhere to the following UB information security and data protection policies in order to provide a secure environment that ensures the privacy and confidentiality of the Data. A brief synopsis of each policy follows. The full policies may be viewed at the links provided.

New York State Information Security Policy

The NY State Information Security Policy, based on ISO17799 standards, developed for state entities, is a comprehensive information security policy. UB has adopted the NY State Information Security Policy as its umbrella computer and information security policy. The policy sets forth the minimum requirements, responsibilities and accepted behaviors to establish and maintain a secure environment and achieve the state's information security objectives.

University at Buffalo Password Policy

All UB passwords must follow the standards contained in this policy. More stringent password standards may be required for access to systems with private regulated data.

University at Buffalo Protection of Regulated Private Data Policy and
University at Buffalo Standards for Securing Regulated Private Data

Extremely sensitive proprietary data, defined as social security numbers, credit/debit card and bank account numbers, state-issued driver's license and non-driver's identification numbers, protected health information, and passwords and other

computer access protection information, are New York State "regulated, private data," subject to this University policy, as well as to the NY State Information Security Breach and Notification Act and other state and federal privacy laws and requirements.

University at Buffalo Data Access and Security Policy

Access to non-public University information is limited to authorized individuals whose jobs require access to the information to perform their assigned duties. Data trustees (access administrators), are responsible for granting and restricting access, and establishing and documenting access authorization. Data custodians (owners) oversee and manage University information resources and policies concerning these resources. Completion of the "UB Access to Information Form" by the authorized individual is required. The Form also requires the signature of his/her supervisor.

BACKGROUND

The Research Foundation central office has issued an *Acceptable Use of Research Foundation Data Outside of RF Business Systems Policy*, providing campus requirements for access to and use of proprietary data considered to be private and confidential by the RF. In order to comply with the RF policy, the University at Buffalo (UB) local acceptable use policy is required to ensure that (1) the University provides a secure environment with proper controls to ensure the privacy, integrity, and confidentiality of extracted proprietary data combined in a non-RF business system and (2) 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: non-proprietary and proprietary

Proprietary Data – RF data that is considered to be private and confidential. Examples include, but are not limited to the following

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

ROLES AND RESPONSIBILITIES

Operations Manager (OM) – Executive Vice President for University Support Services

- Certify that an environment with appropriate policies, procedures, and controls is in place to protect RF data.
- Authorizes access to RF proprietary data consistent with a business need to know
- Utilizing the Access to Non-public Information Form, 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 "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 are 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 the data may also be implemented.

Individuals Authorized to Access Extracted RF Proprietary Data

- Individuals must complete the University at Buffalo Access to Non-public Information 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

Executive Vice President for University Support Services, Operations Manager

501 Capen Hall

University at Buffalo

(716) 645-2901

Information Security Officer

517 Capen Hall

University at Buffalo

sec-office@buffalo.edu