**Rice University Policy No. 808**

# PROTECTION OF UNIVERSITY DATA AND INFORMATION

## I. General Policy

Rice University complies with Federal, State and local laws and regulations related to the protection of confidential and sensitive data, including personally identifiable information, in conducting university business.

This policy applies to all faculty, staff, students, and other individuals working on behalf of Rice University, and covers all confidential or sensitive information related to students, employees, donors, alumni, prospects, applicants, research subjects, and others on whom the university may have such information. The policy applies regardless of how the information is stored (e.g., paper, electronic, cloud, other media) or transmitted.

University data must be appropriately protected at all times, as defined within this policy.

## II. Roles and Responsibilities

All faculty, staff and students who gather, store, transmit, or have access to university data including personally identifiable information are required to treat such information appropriately, and in accordance with this policy and the law. At a minimum this means taking appropriate measures to protect such data, including encryption and password protection.

The Information Technology Security Office provides tools, services, and guidance related to the security of the university's information technology assets. Questions related to these services, as well as questions related to the theft or potential theft of any personally identifiable information (including paper formats), should be directed to the Information Technology Security Office at security@rice.edu.

The Office of General Counsel and the Compliance Office provide guidance for questions related to the treatment of confidential or sensitive information, including: educational records under FERPA; medical or health-related information under HIPAA, the ADA or FMLA; financial information of customers of the university under the GLBA; research related data under relevant laws and agreements; and credit card information obtained and/or maintained under the PCI- DSS.

## III. Definitions

Confidential Information is information or data that is deemed confidential by law, regulation or University policy or which contains information that is highly private or personal or could lead to identity theft if mishandled. Examples of these types of information include, but are not limited to: social security numbers; credit card numbers; driver's license or other government-issued identification numbers; bank account information; protected health information; and student education records (including grades and disciplinary records).

Sensitive Information is information or data that is related to Rice's business and academic activities, although not cloaked with the same level of concern or legal protection as confidential information, is still considered by Rice to be "sensitive information". Examples of these types of information include, but are not limited to: birth dates; home addresses; emergency contact information; employee ID numbers; employee disciplinary records; legal documents (unless publicly disclosed by the University); financial records (unless publicly disclosed by the University); infrastructure information (e.g., IT, physical plant) (unless publicly disclosed by the University).

Personally Identifiable Information is data which is tied to, or otherwise enables identification of, a specific person and makes personal information about them known.

Encryption means any method that will encode data so that it cannot be easily read or understood by unauthorized individuals.

## IV. **Elaboration of Policy**

### A. Confidential Information

University personnel should treat as "Confidential Information" personally identifiable information deemed confidential by law, regulation or University policy or which contains information that is highly private or personal or could lead to identity theft if mishandled. Examples of where this confidential information is located include:

1. Financial Records (e.g., employee loans; donor financial information; student and family financial information including tax returns; payroll records).

2. Health Records (e.g., employee benefit plan information; workers compensation claim information; student medical records; student counseling center information; information regarding disabilities).

Use and release of any such confidential information shall be consistent with law and University policy.

### B. Sensitive Information

Some information related to Rice's business and academic activities, although not cloaked with the same level of concern or legal protection as confidential information, is still considered by Rice to be "sensitive information".

Organizational units must be mindful that while some information may be directory information that would not ordinarily be confidential or sensitive, there may be other reasons for not disclosing the information (e.g., if a student has requested the Registrar not release directory information about that student).

### C. Collection, Storage, Transmission and Disposal of Confidential or Sensitive Data

Each organizational unit of the university is responsible for ensuring that all confidential or sensitive information that is collected, stored, and transmitted is handled in accordance with the following:

1. Collected only as necessary in conjunction with academic and business needs.
2. Restricted in its distribution and accessibility (in some cases approved by a supervisor) as is consistent with good internal control practices, with employees with

access to such information being informed of applicable restrictions.
3. Properly secured by the use of such safeguards as secured file storage and rooms, encryption, and other technology tools (see Section IV.D below).
4. Disposed of through secure means such as shredding and thoroughly erasing hard drives (see Section IV.E below).

Confidential and sensitive information should be shared only on a need-to- know basis and externally only consistent with law. This includes written confidentiality agreements, as appropriate.

If shared internally, colleagues should be informed of the confidential or sensitive nature of the information and the need to safeguard it. If there is any doubt about the appropriateness or prudence of disclosing personally identifiable information, the unit should confer with the Office of General Counsel, Office of Human Resources (for employees), Sponsored Programs and Research Compliance (for research), or the Office of the Registrar (for students).

D. Required Protection of Confidential and Sensitive Information

Any Confidential and Sensitive Information obtained or used by Rice University employees in the performance of their duties, or that is stored on Rice University equipment, computers, or devices, stored in the cloud, or that is stored on a personal device of any type must be appropriately protected at all times. At a minimum, this means that access to the data must require a password or PIN, and that data is properly encrypted while at rest and in transit.

Confidential and Sensitive Information that is kept in a printed format must be adequately secured from authorized access. At a minimum this means that it is stored in a locked office or file cabinet.

Exceptions to this requirement must be approved by the Vice President of Information Technology or Chief Information Security Officer.

E. Disposal of Confidential and Sensitive Information

Confidential and Sensitive Information must be disposed of through secure means such as shredding and thoroughly erasing or destroying hard drives. Employees should be aware that some items such as copiers, faxes and scanners may store protected information which must be erased or destroyed prior to disposal. The Information Technology Security Office is available to assist with appropriate disposal.

F. Traveling with Confidential or Sensitive Information

Employees should exercise caution when traveling with confidential or sensitive data, and only travel with such information when it is necessary to do so. Further, employees should be advised that when traveling to foreign countries certain export control restrictions may apply to certain encryption software (if the software is modified or not commercially available).

The Office of Sponsored Programs and Research Compliance is available to assist you with questions related to export controls.

G. Lost or Misplaced Confidential or Sensitive Information

Anyone who becomes aware that a computer, laptop, mobile device or other equipment containing Confidential or Sensitive information has been lost, stolen, or misplaced must immediately contact the Information Technology Security Office or the Rice University Police Department and report the matter. The Information Technology Security Office will take steps to prevent access, to recover and protect the data, and to assess the extent that data may have been improperly accessed.

## V. Cross References to Related Policies

Policy 832. Appropriate Use of Information Technology

## VI. Responsible Official and Key Offices to Contact Regarding the Policy and its Implementation

Responsible Official: VP Information Technology

Other Key Offices: Office of General Counsel
Sponsored Programs and Research Compliance

*Signed David W. Leebron*
President

Policy History
Revised: October 31, 2017
Issued: February 17, 2011

**Appendix to Policy No. 808– Overview of Various Laws and Regulations relating to Personally Identifiable Information**

1. FERPA—Family Educational Rights and Privacy Act. Limits the disclosure of "education records" defined as those records that are: (a) "directly related" to a student, and, (b) maintained by or on behalf of the university.
   a. A record is "directly related" to a student if it is "personally identifiable" to the student.
   b. A record is "personally identifiable" to a student if it expressly identifies the student by name, address, birth date, social security number, ID number, or other such common identifier.
   c. Examples of "education records" at Rice include registrar records, transcripts, papers, exams, individual class schedules, financial aid records, financial account records, disability accommodation records, disciplinary records, placement records.
   d. "Education records" do not include directory information, unless the student has elected to block the release of directory information.
   e. "Directory information" at Rice includes a student's name, residential addresses, telephone numbers, electronic addresses, date and place of birth, fields of study, dates of attendance, degrees and awards, participation in recognized activities, weight and height of athletic team members, most recent prior educational institution, and a photographic image.
   f. "Education records" also generally do not include certain police records, employment records, health records, or personal memory aid records. Such records may be subject to other regulatory or University policy restrictions.

2. HIPAA—Health Insurance Portability and Accountability Act. Imposes privacy and security standards addressing the use, disclosure, storage and transfer of "protected health information".
   a. "Protected health information" means "individually identifiable health information," which is any information that identifies an individual and relates to the individual's:
      i. Past, present or future physical or mental health or condition,
      ii. Provision of health care, or
      iii. Past, present, or future payment for the provision of health care.
   b. Information is deemed to identify an individual if it could enable someone to determine the individual's identity, such as through an identifier or characteristic that could uniquely identify the individual.
   c. Common identifiers that will make health information "individually identifiable" and therefore deemed "protected health information" include name, address, birth date, social security number, ID number, or other such common identifier.
   d. Examples of information that should be treated as "protected health information" at Rice include employee benefit plan information, worker's compensation claim information, student health services information and student counseling center information.

3. GLBA—Gramm-Leach-Bliley Act. Requires implementation of a written information security program for "customer information."
   a. "Customer information" means any record containing "nonpublic personal information" handled or maintained by or on behalf of the institution about a customer of that institution.
   b. "Nonpublic personal information" includes "personally identifiable information," which in turn is defined as any information:

i. a customer provides to obtain a financial product or service from the institution,
ii. about a customer resulting from any transaction with the institution involving a financial product or service, or
iii. otherwise obtained about a customer in connection with providing a financial product or service to that customer.

c. Common identifiers that will make financial information "personally identifiable" and therefore deemed "customer information" include name, address, birth date, social security number, ID number, or other such common identifier.
d. Examples of "customer information" at Rice include financial records of employees (such as loans), students and their parents (such as cashier's accounts or information related to financial aid), and donors.

4. PCI-DSS –Payment Card Industry Data Security Standards. Requires implementation of security standards surrounding the authorization, processing, storage, and transmission of credit card data. The security standards apply to electronic and paper credit card data.
   a. "Credit card data," as defined by PCI-DSS, is the first six and/or the last four digits of any credit card provided by a customer to conduct University business. If all digits of the credit card are used in the conduct of University business, then name, card expiration date, and source code are considered "credit card data"; and, hence, must be protected.
   b. Examples of operations where PCI-DSS occur on campus include, but are not limited to, Development and Alumni Relations, Parking, the Glasscock School of Continuing Studies, the Jones Graduate School of Business, the Fondren Library, and the Shepherd School of Music, among others, as well as various events and functions for which credit card payments are taken.

5. Texas Identity Theft Enforcement and Protection Act. Requires implementation and maintenance of reasonable procedures to protect information collected or maintained in the regular course of business from unlawful use or disclosure. This includes:
   a. an individual's first name or first initial and last name in combination with at least one of the following identifiers (if the name and the identifier(s) are not encrypted): social security number, driver's license number, government identification number, account number or credit or debit card number along with any required access code; or
   b. information that identifies an individual and relates to the individual's:
      i. physical or mental health or condition,
      ii. provision of health care, or
      iii. payment for the provision of health care.
   c. Publicly available information from federal, state, or local governments is not covered

6. Federal Freedom of Information Act or to the Texas Open Records Act. As a private institution, Rice is generally not subject to the Federal Freedom of Information Act or the Texas Open Records Act. Inquiry may be made by contacting the Office of General Counsel.