RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.1.2

Section Title: Information Technology Policies

Policy Name: Information Classification

Formerly Book: Former Policy 70.2.2

Approval Authority: Senior Vice President for Administration

Responsible Executive: Vice President for Information Technology and Chief Information Officer

Responsible Office: Office of Information Technology (OIT)

Originally Issued: July 1, 2013

Revisions: Originally 00-01-95-15:10 at UMDNJ; 10/10/2013 (Updated title), 7/3/2014 (Significant updates)

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**
   This policy outlines the standards for classifying information at Rutgers, The State University of New Jersey. Classification categories (Restricted, Internal and Public) are provided and defined in order to ensure protection of University data is consistent with all applicable laws and regulations, particularly with respect to protected health information.

2. **Reason for Policy**
   To ensure that University information is properly identified and classified, and handled according to its value, legal requirements, sensitivity, and criticality to the University. To ensure that University information receives appropriate and consistent levels of protection to safeguard its confidentiality, integrity, and availability.

3. **Who Should Read This Policy**
   Parties with major responsibilities include Vice Presidents, Chancellors, Deans, Information Owners (data custodians), Information Managers and Information Users. This policy applies to all members of the University community including faculty, staff, students, covered entities, contractors, non-employees, and agents of the University.

4. **Related Documents**
   Policies.rutgers.edu: Information Technology - Section 70
   Policies.rutgers.edu: Clinical, Compliance, Ethics & Corporate Integrity - Section 100
   Policies.rutgers.edu: Payment Card Acceptance Policy, 40.2.15
   Policies.rutgers.edu: Copyright Policy, Section 50.3.7
   Policies.rutgers.edu: Identity Theft Compliance Policy, Section 50.3.9
   Policies.rutgers.edu: Records Management, 30.4.5
   Policies.rutgers.edu: Gramm-Leach-Bliley Act (GLBA) Information Security Policy, 50.3.11
   Policies.rutgers.edu: Red Flag Detection and Reporting Policy, 50.3.12
   OIT Policies Website: http://oit.rutgers.edu/policies
   RU Secure Website: http://rusecure.rutgers.edu/
   Rutgers Minimum Security Standards for Data Protection http://rusecure.rutgers.edu/policies

5. **Contacts**

Information Protection and Security, Office of Information Technology
848-445-8011
http://rusecure.rutgers.edu

6. **The Policy**

70.1.2 INFORMATION CLASSIFICATION

A. Introduction:

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of University information collected, processed, stored, or transmitted irrespective of the location or medium on which the information resides. Confidentiality, integrity, and availability are defined as follows:

- Confidentiality – the expectation that only authorized individuals, processes, and systems will have access to University information.
- Integrity – the expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.
- Availability – the expectation that information is accessible by the University community when needed.

Information must be classified and handled according to its value, legal requirements, sensitivity, and criticality to the University. Protection levels must be established and implemented relative to the information's classification, ensuring against unauthorized access, modification, disclosure, and destruction. For information governed by law and regulations (such as student records, personally identifiable information and protected health information), the protection levels must satisfy the respective, data security and data privacy requirements (e.g., FERPA, HIPAA).

B. Requirements:

1.) Vice Presidents, Chancellors and Deans must:

a. Ensure that each business unit in their respective areas of oversight appropriately identify and classify information generated, accessed and stored by the business unit.

b. Ensure that each member of their business units receives periodic training and awareness about how to handle Restricted information.

c. Assign business unit managers, senior managers, or designees the role of "Information Owner (data custodians)" for their respective areas. Ensure that their information owners (data custodians) maintain an inventory of their information assets, including applications.

d. Annually perform a risk assessment of their applications and data. For areas with specific compliance and regulatory requirements such as HIPAA and GLBA, business units must also report their aggregate inventory of information assets to OIT Information Protection and Security.

e. Ensure through appropriate "due diligence" and contract terms that contracted vendors have an appropriate level of assurance to protect University data.

2.) Information Owners (data custodians) must:

a. Classify University information under their control as:

- Restricted
- Internal
- Public

Such classifications shall be conducted in accordance with the guidance set forth in the Information Classification Table at the end of this policy.

They should take into consideration the business needs and legal requirements for sharing or restricting information and the impacts associated with those needs and requirements.

b. Clearly identify Restricted and Internal Information specially when sharing or providing individuals, departments or third parties with access.

c. Establish the business unit's security requirements and expectations for the applications the business unit owns and which contain their information. For example:
   i. How a user should be authenticated.
   ii. How users will be granted access to the application and/or information.
   iii. Revocation procedures of user access privileges.
   iv. Procedures for approving requests for access and use of the information in its applications.
   v. Record retention and e-discovery requirements.

d. Provide training and awareness about information handling to users with access to their Restricted Information.

e. Maintain an inventory of their information assets, including all applications that collect, process, store, or transmit their information.

f. Conduct an annual entitlement review of individuals, departments and third parties who have been granted access to Restricted information.

g. At minimum, annually assess and update the Information Classification, based on changing usage, sensitivities, law, or other relevant circumstances.

h. Establish procedures for data destruction in accordance with the University's records retention and disposal policies. See policy 30.4.5 Records Management.

i. Annually perform a risk assessment of their applications and information and revise the unit's requirements as needed to address changing University requirements, changes in law and as a result of changing risks.

j. Ensure Information Users are aware of and apply the "Rutgers Minimum Security Standards for Data Protection" (e.g. Restricted data must be encrypted on mobile devices and when transmitted).

k. Ensure compliance with regulatory requirements such as HIPAA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach-Bliley Act), PCI (Payment Card Industry) and other state, federal, and contractual requirements that may apply. See the Related Documents Section for further information.

3.) Information Users must:

a. Receive approval from the Information Owner (data custodians) prior to accessing Restricted or Internal information.

b. Adhere to the Information Owner's (data custodian's) security requirements and safeguards.

c. Not re-disseminate Restricted or Internal information to which they have been granted access without authorization from the Information Owner (data custodians).

d. Apply the **"**Rutgers Minimum Security Standards for Data Protection" as appropriate based on the data classification.

4.) External Data Handling Security Requirements:

Information entrusted to the University by grant-providers, other universities or other agencies (DoD, NEH, NIH, NSF or similar) must be protected, at minimum, according to contractual obligations, regulatory requirements, and/or University policy, and relative to the sensitivity of the information.

5.) Internal Data provided to External (third party) Services:

a. No Restricted or Internal information may be provided outside of the department or outside of the university until an agreement is put in place. Contracts with third party service providers shall include a "HIPAA Business Associates Agreement" or Purchasing's "Contract Addendum Concerning Protected Information."

b. University Restricted and Internal information provided to outside or "cloud" (third party) service providers must be protected by the third party at least at the level that it would be protected by the University and federal regulations. For PHI data (defined in the appendix), a HIPAA Business Associates Agreement is required. Information Protection and Security must review the third party service agreement prior to the contract being signed if the service involves Restricted information.

C Information Security Incident Reporting

Unauthorized use, disclosure, loss or theft of Restricted or Internal information must be reported immediately. The following steps must be taken:

1.) Immediately report the unauthorized disclosure, loss, theft, or access to information to Information Protection and Security, OIT and your departmental management.
2.) If PHI or there is a likelihood that PHI data is involved, Call the Rutgers Hotline (1-800-215-9664).
3.) Report loss or theft of physical assets to University Police. If PHI or there is a likelihood that PHI data is involved, Call the Rutgers Hotline.

D. Non-Compliance and Sanctions

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable state and federal statutes.

E. Appendix

Information Classification Table

Appendix

Information Classification Table

Please see Rutgers Minimum Security Standards for Data Protection which outlines the minimum level of controls necessary for each category. https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection

Information Classification	Description	Examples
Restricted	Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as 'non-public personal information' (NPPI) about people or critical business, academic or research operations under the purview of the Information Owner (Data Custodian). Restricted data includes, but is not limited to, data that University is required to protect under regulatory or legal requirements. Unauthorized disclosure or access may 1) subject Rutgers to legal risk, 2) adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA penalties).	• Bank information • Login Credentials (username & password) • Credit/Debit Card Number • Driver's License Number • Human Resources information if it contains SSNs, medical reports, etc. • Passport Number • Protected Health Care Information (PHI)[1] • Protected Data Related to Research[2] • Social Security Number • Student Disciplinary, or Judicial Action Information • Police Records • Student Records (FERPA)
Internal	All other non-public information not included in the Restricted category.	• Licensed Software • Other University Owned Non-Public Data • University Identification Number or Information Number (employee numbers, student ID numbers, etc.)
Public	All public information.	General access data, such as that on unauthenticated portions of any rutgers.edu site.

[1]Protected Health Care Information includes, but is not limited, to the following:

- Protected Health Information (PHI) or Electronic Protected Health Information (EPHI)
- Patient health-care and human subjects research records
- Payment transactions related to health services
- Medical and personal information in research records
- Quality-assurance and peer-review information from patient care units

[2]Protected Data Related to Research

- University proprietary information, including copyrightable and patentable information
- Proprietary information belonging to other individuals or entities, such as under a non-disclosure agreement or contract
- Library circulation records and any information about use of any library information resource in any format